A Review of Evidence Relating to Harm Resulting from Uses of Health and Biomedical Data

Prepared for the Nuffield Council on Bioethics Working Party on Biological and Health Data and the Expert Advisory Group on Data Access by:

Professor Graeme Laurie,
University of Edinburgh

Dr Kerina H. Jones,
Swansea University

Ms Leslie Stevens,
University of Edinburgh

Dr Christine Dobbs,
Swansea University

30 June 2014

We would like to take this opportunity to thank the NCOB *Working Party on Biological and Health Data* and the *EAGDA* Secretariat for their helpful comments in finalising this report, and to Cameron Kennedy for his research assistance at this final stage.

LIST OF TABLES 8

LIST OF FIGURES 9

EXECUTIVE SUMMARY 10

1. METHODOLOGY/APPROACH 14

1.A Background to the evidence review 14

1.B Scope 15

1.C Methodology/Approach 17

1.C.1 Research design 17

1.C.2 Search type 18

1.D Limitations 19

1.D.1 Care.data 21

1.D.2 Limitations inherent to the judicial and regulatory system 21

2. INTRODUCTION 23

2.A Context of the evidence review 23

2.B Research questions and pathways to answers 26

3. DEFINITIONS AND INITIAL CLASSIFICATIONS OF ABUSE, CAUSE FOR ABUSE AND HARM 28

3.A The regulation of health and biomedical data 28

3.A.1 Personal and sensitive personal data under the DPA 29

3.A.2 Identifiability and de-identification of data 31

3.B Harm under data protection law – harm as damage or distress 35

3.B.1 Preventative measures of redress under the DPA 35

3.B.2 Seeking redress *post*-harm under the DPA 36

3.B.2.A Non-compensatory redress under the DPA 36

3.B.2.B Compensation under the DPA 37

3.B.3 Final thoughts on the legal notion of harm under the DPA 39

3.B.3.1 Harms to the public interest or organisations 39

3.B.3.2 Redressing 'harm' to broader, public interests under the DPA 40

3.C Harm in other contexts 41

3.C.1 Personal identity and coping mechanisms 42

3.C.2 Social identity and vulnerable social groups 42
3.C.3 Higher-power/higher-status groups 43
3.C.4 Lower-power/lower-status groups 43
3.C.5 Perpetrators and prejudice/discrimination 44
3.C.6 The harm versus the impact 44
3.C.7 Impact in the psychosocial context 45

4. ABUSE AND HARM – CATEGORIES, CAUSES AND IMPACT 47

4.A Categories of abuse 48

4.B Causes for abuse 49

4.C Harm types 50

5. APPROACH/METHODOLOGY 52

6. METHOD 52

6.A Hard evidence 52

6.B Soft evidence 53

6.C Twitter evidence 57

7. RESULTS 58

7.A Initial findings 58
7.A.1 Hard Evidence 58
7.A.2 Soft evidence 60
7.A.2.A Newspapers 60
7.A.2.B Charities and citizens' voice groups 62
7.A.3 Twitter Evidence 64

7.B Typologies of abuse by cause and abuse by harm/impact 65
7.B.1 Hard evidence typology 65
7.B.1.A Inconsistent reporting across UK and European judgments 65
7.B.1.B Frequencies of abuse reported in the hard evidence 66
7.B.1.C Incidence of abuse involving DNA profiles and tissue 69
7.B.1.D Frequencies of abuse by harm reported in the hard evidence 70
7.B.1.E Potential harm 72
7.B.1.F Findings of actual harm 73
7.B.1.E Findings of 'no' harm or where there was 'no evidence of harm' 74
7.B.1.F Harm arising from non-use of data 74
7.B.1.G Harm to broader public interests 75

7.B.2 Soft evidence typology 77
7.B.2.A Abuse by cause typology 77
7.B.2.A.1 Incidents involving NHS Staff 77
7.B.2.A.2 The motivations behind the incidents involving NHS Staff 81
7.B.2.A.3 Incidents involving individuals outside of the NHS 82
7.B.2.A.4 Breaches facilitated by maladministration or human error – borderline cases 83
7.B.2.B Abuse by Impact typology 83
7.B.2.B.1 Harm caused through falsification/fabrication 85
7.B.2.B.2 Impact of harm caused through human error 86
7.B.2.B.3 Impact of harm caused by unauthorised/inappropriate disclosure or retention 87
7.B.3 Twitter evidence typology 87
7.B.3.A Frequencies of abuse reported in the Twitter evidence 87
7.B.3.B Theft 89
7.B.3.C Unauthorised disclosure or access 90
7.B.3.D Technical security failures 91
7.B.3.E Other motivations for abuse 93
7.B.3.F Categories of harm in the Twitter evidence 93
7.B.3.G Potential harm 95
7.B.3.H Actual harm 95
7.B.3.I No harm – but compensation 95

7.C Merged evidence 96
7.C.1 Overlap between hard and soft evidence 96
7.C.2 Overlap between hard, soft and Twitter evidence 96
7.C.3 Useful comparisons between the evidence strands 97

8. CONCLUSIONS 98

8.A Conclusions drawn from the hard evidence 98
8.A.1 Evidence of individual impact lacking 98
8.A.2 Understanding risks for harm – actual versus potential harm 98
8.A.3 Harms to the public interest 99
8.A.4 Harms outwith privacy harms 100

8.B Soft evidence 101
8.B.1 Abuse in the biomedical and healthcare sectors 101
8.B.2 Types of abuse 102
8.B.3 Causes of abuse – the motivations to abuse 103
8.B.4 Facilitation of abuse – maladministration and human error 103
8.B.5 Impacts of abuse 104
8.B.6 Quality of findings in newspapers 105
8.B.7 Quality of findings in charities and citizens' voice groups 107

8.C Conclusions drawn from Twitter evidence 108

8.C.1 Prevalent abuse types 108
8.C.1.A Misconceptions on level of harm uncovered 110

9. IMPLICATIONS OF THE EVIDENCE 112

9.A Implications for governance 112
9.A.1 Maladministration (most prevalent cause for abuse) 113
9.A.2 Processing against individual objections or without their consent 116
9.A.2.A Legal obligations and good governance 117
9.A.3 Unauthorised disclosure by the press 118
9.A.4 Unauthorised access due to insufficient safeguards 119
9.A.5 Human error 120
9.A.6 Falsification and fabrication 121
9.A.7 Genetic data 122
9.A.7.A S and Marper v United Kingdom 122
9.A.8 Non-use of data 126
9.A.8.A Focus of this section 126
9.A.8.B Context 126
9.A.8.C Clinical records 127
9.A.8.D Research data 129
9.A.8.E Governance frameworks 131
9.A.8.F Conclusions on non-use 135
9.A.9 Conclusions on the implications for governance 136

9.B Assessing the effectiveness of sanctions and remedies in light the prevalence of abuse uncovered 137
9.B.1 Sanctions 137
9.B.1.A ICO Sanctions 138
9.B.1.B First-tier Tribunal (Information Rights) Judgments 140
9.B.1.C UK Court Judgments 140
9.B.1.D European Court Judgments 141
9.B.2 Overall effectiveness of sanctions for abuse of health or biomedical data 141

9.C Remedies 142
9.C.1 Overall effectiveness of remedies for abuse of health or biomedical data 144

9.D Addressing incentives and disincentives to abuse 144
9.D.1 The black market for data 144
9.D.2 Re-identification attacks 147
9.D.3 Disincentives 148
9.D.3.A The repeat offender 148
9.D.3.B Other ‘offenders’ 149
9.D.3.B.1 Staff who have acted with intent but who have the ability to learn from the experience 149

9.D.3.B.2 Staff where abuse was unintentional 151
9.D.3.C Data protection awareness (re-)training – bringing home the real-life message 152
9.D.3.D Our cautionary tale 153
9.D.4 Conclusions on motivations 156

10. FUTURE RESEARCH 157

10.A Widening the sources searched and reducing the scope 157

10.B Future research on social constructionism 158

10.C Future Research on Non-Use 159

10.D Future research on genetic data 159

10.E Future research on the risks, threats and vulnerabilities in processing health and biomedical data 160

10.F Future research and the necessity of public debate 160

11. CONCLUDING THOUGHTS 161

APPENDICES 163

List of Tables

Table 1: Legal databases and websites 16
Table 2: Soft evidence – list of newspaper, charity and citizens' voice websites 16
Table 3: Number of breaches in Q3 2013 by sector 23
Table 4: Hard evidence: websites consulted 53
Table 5: Soft evidence – list of newspaper, charity and citizens' voice websites 53
Table 6: Newspapers, charities and citizen's voice groups 55
Table 7: Hard evidence results 58
Table 8: Search conditions and hits by newspaper 61
Table 9: Post-scrutiny abuse hits from January 2009 to March 2014 by newspaper by year 62
Table 10: Hits by charity and citizens' voice groups 63
Table 11: Twitter hits using advanced search 64
Table 12: Hard evidence – Abuse by cause 67
Table 13: Hard evidence – Abuse by harm 71
Table 14: Soft evidence: Abuse by cause 78
Table 15: Determinable motivations behind all incidents involving NHS Staff 81
Table 16: Soft evidence: Abuse by impact 84
Table 17: Twitter evidence – Abuse by cause 88
Table 18: Twitter – Abuse by Harm 94
Table 19: Discourse analysis – Telegraph and Guardian 106
Table 20: Discourse analysis – Telegraph and Independent 107
Table 21: Alternative websites – Overview of hits and relevance 158
Table 22: Full details of hard evidence search 164
Table 23: Hard evidence incidents 166
Table 24: Social media evidence of health or biomedical data abuse internationally 181
Table 25: Soft newspaper evidence incidents 194
Table 26: Impact statements from newspaper articles 201
Table 27: Reference List for newspaper articles 203
Table 28: Journals, trade magazines and blogs future research search 208

List of Figures

Figure 1: Searches for the three evidence strands 19
Figure 2: Health sector – Q1 to Q3 trends in 2013 24
Figure 3: Harm in the context of the hard and the soft evidence searches 47
Figure 4: Types of abuse 48
Figure 5: Causes for abuse of data 49
Figure 6: Harms caused by abuse 50
Figure 7: Overlapping reporting of incidents 96
Figure 8: Soft evidence – Types of abuse 102
Figure 9: Comparing types of abuse across the three evidence strands 103
Figure 10:Comparing frequencies of impact/harm across the three evidence strands 104
Figure 11:Comparing reading levels across three newspapers 105
Figure 12: Spectrum of sanctions uncovered in the evidence review 137
Figure 13: Remedies identified in the evidence review 142
Figure 14: The data protection landscape in the UK (simplified) 154

Executive Summary

The Nuffield Council on Bioethics (NCOB) *Working Party on Biological and Health Data* and the *Expert Advisory Group on Data Access* (EAGDA) commissioned this evidence review entitled *Review of evidence relating to harms resulting from security breaches or infringements of privacy involving sensitive personal biomedical and health data (including any knock-on effects on beneficial data sharing).* The purpose for the evidence review was to allow the NCOB and EAGDA to better understand, for example: the nature of the actual harms resulting from data misuse or security breaches involving sensitive personal biomedical and health data; the relevant, regulatory definitions; the appropriate context in which to assess harm; the effectiveness of sanctions and remedies; and the opportunity costs to institutions or individuals of not sharing or linking data. The scope was broad with a tight timeframe (February-April 2014). This piece of work was to be regarded as a scoping exercise and the approach was as follows:

1. The research: This research was conducted by a multi-disciplinary team from the Mason Institute at University of Edinburgh's School of Law and the Farr Institute's CIPHER based at Swansea University's College of Medicine. Evidence was sought from three types of source; legal websites ('hard evidence'), websites of newspapers, charities and citizens' voice groups ('soft evidence'), and the social media site Twitter. Each piece of evidence was examined to establish where possible the category 'type' of abuse (e.g. non-secure disposal), the category 'cause' of the abuse (e.g. to meet NHS targets) and the resultant category 'harm' (e.g. individual distress). Because the evidence was in the form of unstructured, qualitative data, thematic content analysis was undertaken. One limitation of this analysis tool is that some categories were broad (e.g. maladministration, human error).

2. Terms of Reference: Because the scope of the review examined evidence in the regulatory and psychosocial contexts, there were some definitions that were context-dependent. The regulatory definitions that apply to the protection of sensitive, personal biomedical and health data set the parameters. There is, however, a distinction between hard evidence *harms* as defined by the law and legal institutions that set the thresholds high and soft evidence *impacts*, the subjective affect that is triggered by a harm.

3. The added value of three sets of findings. Hard evidence findings contributed greatly to our understanding of the types of circumstance that lead to abuse of health or biomedical data, and especially for governance concerns. However, what was often lacking was insight into the individuals' perspective on the abuse and harm/impact. Harm to broader public interests, such as loss of public trust in public bodies such as the NHS or in the confidentiality of doctor-patient relations are simply not provided for in law. **Soft evidence findings** illustrated well the real psychosocial and social impact that an instance of harm can have on an individual and their significant others. Here and only here evidence was found regarding the impact of falsification/fabrication of patient data. **Twitter evidence findings** were US-centric. As such, the incidents offered good insight into general data breach trends and a contrast to the UK-based results, which offered more insight into governance. Theft was found to be far more common in the US, whereas non-secure disposal of data was more prevalent in the UK.

4. Implications and recommendations for Governance: The number one cause contributing to abuse of health and biomedical data was maladministration, which can also be understood as the epitome of poor governance practices. **Key recommendation:** Thus there is an apparent

need for improvement over the effective monitoring of personnel, and standards and procedures that are already in place in the NHS and other healthcare organisations. This includes: a need for random spot checks for compliance; robust auditing procedures for how data are accessed, transferred and generally used on and off premises; and specific guidance on particular uses of data and especially for more sensitive data (e.g. faxes, emails, use of portable media etc.).

However, there is an equal need to be wary of simply adding more bureaucratic burdens specifically on the NHS. Governance must be fit-for-purpose and proportionate. Where there are failings, underlying systemic organisational issues need to be identified. **Key recommendation:** Where there are failings that lead to abuse of health and biomedical data, a 360° appraisal of the organisation will identify more precisely where weaknesses lie.

Mere compliance to legal rules or official guidance might not be enough to secure the social licence required for trusted and effective data use, linkage, sharing and transfer. A governance system that shows awareness of, and responsiveness to, likely impacts of data management is more likely to meet this objective. **Key recommendation:** Among other things, on-going and transparent engagement with data subjects and public groups is central. Such engagement must show a true willingness to engage in dialogue and a demonstrated ability to learn from the public experience.

5. Implications and recommendations for Sanctions and Remedies: The evidence shows a narrow range of sanctions available when health or biomedical data have been abused. The sanctions available are not entirely ineffective, but equally they are not fully capable of offering robust disincentives for further abuse. As a large portion of abuses are addressed at an earlier stage of a complaints process or otherwise go unreported, it is not possible to assess the effectiveness of a potentially wide portion of 'sanctions' available. The effectiveness of sanctions imposed at *later* stages (usually post-abuse) is limited in the UK. In this regard, the European Court of Human Rights (ECtHR) serves an extremely important role in providing an alternative forum to address abuses that could be overlooked within any domestic system. **Key recommendation:** The ECtHR makes important contributions to how the UK should conceptualise the notion of privacy and concomitantly protect against prospective violations of individuals' Article 8 rights, outwith the more narrow confines of the Data Protection Act 1998.

Our assessment of the limited scope of *legal* remedies is, nonetheless, complemented by our broader understanding and conceptualisation of harm and impact. Given that the abuse of data can result in multiple types of harm (financial, legal, physical, social, and psychological), the prevention of harmful processing and/or award of damages can only address a small aspect of harm caused to individuals. Furthermore, these remedies cannot rectify harm caused to broader public interests such as diminishment of public trust in the health services they receive or in the confidentiality of relationships e.g. between doctors and patients. The overall effectiveness of remedies for harm is considered *ineffective* given the broader understanding of harm provided for in this report. **Key recommendation:** Earlier and closer attention must be paid to the identification of the range of interests at stake. This should include more explicit engagement with all population groups, but particularly with hard-to-reach groups, and an enacted recognition of their sensitivities within governance mechanisms.

6. The cost of non-use of data and recommendations: This review produced little/no proven instances of harm due to the non-use of data, and this is indicative of how elusive it is to prove non-use, and thus determine the cost of opportunities lost. Further, harm due to non-use of data is not simply the opposite of benefit due to data use. There are a considerable number of multi-faceted reasons for this. **Non-use of clinical records**: non-entry of data; input errors; the complexities of coding. **Non-use in research:** publication bias; researchers and organisations

unwillingness to share data; pharmaceutical companies wanting to present only positive results. Non-use through Governance: Governance too plays a role in the lack of data sharing, where particular pieces of legislation or regulation have been criticised for over-caution. Without disputing in any way the necessity and correctness of Governance, there is a heightened risk of clinical error through a lack of joined-up information. Non-use of data can have far-reaching consequences for the patient's care, for the healthcare professional, for the future of medical advancement and for the NHS economically. We have addressed above that Governance alone cannot always ensure correct data usage. **Key recommendation:** We strongly recommend further research, including listening to data handlers', researchers' and healthcare practitioners' stories, that give more insights into the cost of opportunities lost.

7. Incentives and disincentives to misuse and recommendations: Incentives: Causes for abuse were identified in the search, and a section considered the prospect for large-scale abuse such as found on the data black market, and in re-identification attacks. Although no direct evidence was found in these fields in the UK, the importance of constant vigilance remains given the potential economic and professional motives that might drive such attempts for abuse.

Disincentives: It was suggested that there are, broadly, three types of 'offender'. The first is incorrigible; there is little likelihood of correcting such behaviour and future intentions. Here, harsh sanctions are necessary up to and including dismissal. The second offender type has acted intentionally, but attitude and behaviour change is possible. The third is the unintentional offender. **Key recommendations**: For types two and three offenders, the action must be considered in context. It is crucial that these individuals can speak without fear about their motivations, which must be established clearly in order to put the best and most appropriate corrective measure in place. Corrective measures should aim to foster conformity (attitude and behaviour changes) and not compliance (only behaviour changes, the attitude regarding abuse/misuse of data remains). Re-training measures should reflect real-life situations, such as group work with patient stories.

8. Future research: The evidence review highlighted several areas where further research would be warranted outwith the scope and limitations of this report. We strongly recommend reducing the scope of any piece of future work, giving opportunity to explore in-depth and exhaustively. Here we provide indications of the topic and nature of potential areas of interest for both NCOB and EAGDA in future.

- The deeper exploration of sub-categories where our methodological design and scoping exercise have identified areas of particular concern regarding the abuse/misuse of health and biomedical data, such as 'maladministration' and 'human error'.

- Depending on the topic under investigation, an array of other sources could be drawn up in the evidence gathering phase. We have provided an example of alternative sources and their potential as an evidence source.

- Based on the extensive findings from newspapers, future research examining the social construction of issues around health data misuse and abuse, and the symbiotic relationship between the media and the public would contribute to an understanding of the wider, social context of data protection.

- Establishing the opportunities lost due to non-use of biomedical and health data is elusive. There would be value in a prospective study to identify, and supply more robust evidence

on, causes of data non-use in research There would be value in a prospective study to identify, and supply more robust evidence on, causes of data non-use in research. A piece of research similar to this review – examining abuse and misuse of **genetic data** – more narrowly defined and therefore more in-depth.

- Further examination of risks, threats and vulnerabilities in processing health and biomedical data *prior* to harm/abuse. This could be a series of qualitative, in-depth interviews with data controllers and other personnel from selected sites

- Opening the debate to the wider public, perhaps in the form of consultation workshops and as a qualitative piece of research.

1. Methodology/Approach

1.A Background to the evidence review

The Nuffield Council on Bioethics (NCOB) Working Party on Biological and Health Data and the Expert Advisory Group on Data Access (EAGDA) commissioned this evidence review. The tender provided for a final report of approximately 15,000 – 20,000 words, with a turn-around time of eight weeks. The purpose for the evidence review was to allow the NCOB and EAGDA to better understand:

a) the nature of the actual harms resulting from data misuse or security breaches involving sensitive personal biomedical and health data,
b) the relevant, regulatory definitions,
c) the nature and significance of any conditions incentivising misuse of data,
d) how the incidence and prevalence of such harms is assessed,
e) the inherent limitations to methodologies of assessment,
f) the appropriate context in which to assess harm,
g) the robustness of available governance mechanisms,
h) the effectiveness of sanctions and remedies and
i) the opportunity costs to institutions or individuals of not sharing or linking data.

In winning the bid competitively, a multi-disciplinary team was formed between the Mason Institute at the University of Edinburgh's School of Law[1] and Farr Institute's CIPHER[2] at Swansea University's College of Medicine.

The multi-disciplinary remit was extensive, and included:

1. an overview of the relevant regulatory definitions of data, harm and abuse,
2. consideration of 'abuse' in the psychosocial context,
3. a bespoke, methodological design to undertake a three-stranded evidence review,
4. the undertaking of said research,
5. the development of a series of typologies of harm and abuse,
6. a comparison of the evidence between and within the three evidence strands,
7. drawing conclusions from each evidence strand and
8. a discussion of the implications of these findings in the wider legal, social and psychological contexts.

[1] The Mason Institute <http://masoninstitute.org/> accessed 10 June 2014.
[2] The Farr Institute at CIPHER <http://www.farrinstitute.org/centre/CIPHER/34_About.html> accessed 10 June 2014.

This was, therefore, an ambitious project and, to our knowledge, the marrying of findings from the three evidence strands (the legal perspective, the grey literature and Twitter) has not been attempted before. Against this backdrop and especially in light of the timescales involved, the review was understood as a *scoping* exercise, not an exhaustive evidence review. Further and as per the Brief for Tender, the focus was to be UK-centric in the main, looking beyond to a lesser degree.

We operated under extremely tight time-constraints, which did not come at the price of academic rigor. Ultimately a report of 71620 word length emerged. Post-review we now include Section 10 *Future Research* where we address important issues and questions that emerged from this scoping exercise.

1.B Scope

The review was undertaken using a multi-disciplinary approach encompassing the disciplines of law and social psychology, as well as areas of expertise around information governance and data linkage security. The legal expertise was in the fields of medical law, jurisprudence, ethics and data protection, ensuring that there was a firm understanding of the tenets and legislation on which data protection and other legal issues in the health and biomedical context are founded. Expertise in information governance and data linkages gave the team a firm basis regarding the translation of law into governance, additionally with a high awareness of potential hazards regarding security breaches. Expertise in social psychology brought a humanistic understanding into play, which enabled speculations on individuals' and social groups' motivations, fears and behaviours from the standpoint of the perpetrator and the subject.

The *Introduction* (Section 2.A Context of the evidence review) provided the contextual backdrop to the evidence review in light of the core questions guiding the review. This section concluded with the research questions and our pathway to answering these. Section 3.A offered an overview of the regulation of health and biomedical data in the UK, setting the definitional parameters for the review on health and biomedical data as understood within the UK and EU's regulatory context. Relevant conceptions of harm were also discussed, in the narrow, legal context as well as the broader, psychosocial context.

Section 6 *Method* discusses the specific search parameters for each of the three evidence strands – legal, grey literature and Twitter – each with its own scope.

The legal databases ('hard' evidence) searched were:

Table 1: Legal databases and websites

Site	Time frame	Search terms
UK Case Law within LexisNexis: **http://www.lexisnexis.com/uk/legal/**	1998-2014	'health or medical PRE/1 data and breach' 'biomedical and data' 'biological data' 'genetic and data and breach' 'health and data and non-use'
UK Information Tribunal Cases: **http://www.informationtribunal.gov.uk/Public/search.aspx**	-	**jurisdictional area 'DPA 1998'** 'sensitive personal data' 'confidentiality of information' 'right to prevent processing likely to cause damage or distress' **jurisdictional area 'HRA 1998'** 'right to private and family life' **jurisdictional area 'FOI 2000'** 'information provided in confidence'
UK Information Commissioner's Office Prosecutions, Monetary Penalty Notices and Decision Notices: **http://ico.org.uk/enforcement**	-	**Prosecutions and Monetary Penalty Notices:** no search terms used; read case by case **Decision Notices:** 'health data', 'biomedical data'
EU Case Law within LexisNexis: **http://www.lexisnexis.com/uk/legal/**	1995-2014	'health or medical PRE/1 data and breach' 'genetic or biomedical and data and breach' 'biological data' 'health and data and non-use'

The grey literature search ('soft' evidence) consulted:

Table 2: Soft evidence – list of newspaper, charity and citizens' voice websites

Newspapers	**Charities**	**'Citizens' Voice'**
Express	Age UK	Big Brother Watch
Guardian	Carers UK	Citizen's Advice
Independent	Lesbian and Gay Foundation	Digital Right Ireland
Mail	Mind	GeneWatch
Mirror	Prisoners' Advice Service	Healthwatch
Sun	Prison Reform Trust	Liberty
Telegraph	Race Equality First	medConfidential
Times	Race Equality Foundation	Patients' Association
Belfast Telegraph (NI)	Stonewall	Patient Care (Watchdog)
The Herald (Scotland)	Terrence Higgins Trust	Patient Concern
Western Mail (Wales)		
Search terms*	**Search terms***	**Search terms***
medical; *patient*; *record*; *data*; *breach*; *misuse*; *biomedic*; *genetic*	*data, breach* and/or *misuse*	*data, breach* and/or *misuse*

*Because these were only in part possible using Boolean operators, we do not include any search terms in single brackets

The Twitter evidence search:

We also searched the social media website Twitter (after excluding Facebook as a viable search tool). Twitter's advanced search function was employed for the terms 'health data breach', excluding the words 'care.data'. This search returned over 1,000 hits, whilst the search for 'biomedical data breach', 'biological data' and 'genetic data breach' (excluding 'care.data) returned zero results.[3] The search was revised to search for: 'medical data breach', excluding the words 'care.data' and limiting the search to tweets posted within Scotland, UK.[4]

1.C Methodology/Approach

This section addresses the methodology of the research design, and the choice of search type.

1.C.1 Research design

To our knowledge this was the first piece of work aiming to compare 'hard' and 'soft' evidence and evidence from social media (Twitter).[5] The evidence uncovered was in the form of raw, qualitative data that posed difficulties in making comparisons in terms of specific languages used (e.g. legal, newspaper articles from broadsheets to tabloids, the demographic diversity of tweeters). Therefore we rejected taking a top-down, deductive approach, because this would have meant that we had pre-conceived ideas of what we would find. Rather, we chose a bottom-up, inductive approach. This was crucial in order to keep an open mind as to what sorts of evidence would emerge, and this was the most auspicious way to be able to later compare and contrast findings between the evidence strands.

The goal was to collapse our findings (raw, textual data) into short summaries of each event or incident, and then to assess and group together summaries that were similar.[6] This was first performed within each strand (see e.g. Section 7.A.1 Hard Evidence) and then between the strands (see Section 7.C Merged evidence).

Team discussions were held to create the best labels for these groups of summaries (categories and sub-categories). This was a cyclic, non-linear and iterative process. It is generally acknowledged that one should develop as many valid and reliable categories as are

[3] Due to space constraints and to facilitate data analysis the search was narrowed.

[4] Scotland, UK as opposed to the entirety of the UK was chosen as the limiting variable to the search because it was not possible to select tweets posted from within the whole UK – only specific cities, zip codes or countries.

[5] Please see Section 2.B Research questions and pathways to answers for the rationale behind our approach.

[6] See for example: David R Thomas, 'A General Inductive Approach for Analyzing Qualitative Evaluation Data' (2006) American Journal of Evaluation, 27(2), 237-246; Virginia Braun and Victoria Clarke, 'Using thematic analysis in psychology', (2006) Qualitative Research in Psychology 3 (2) 77-101; Jennifer Fereday and Eimear Muir-Cochrane, 'Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development' (2006) International Journal of Qualitative Methods 5(1) 80-92; Richard E Boyatzis, *Transforming qualitative information: Thematic analysis and code development* (Sage 1998).

necessary, but only as many as would pass scrutiny. By using this method we were able to create the typologies of, for example, *abuse by cause* (see Table 12 and Table 14).

1.C.2 Search type

This section will detail fully how we conducted our searches and under what conditions to ensure transparency, thus allowing the interested reader the option to replicate the study.

There were three stages in our approach to identifying evidence of harm (see Figure 1 below).

Stage one comprised three searches. These were undertaken in parallel and employed systematic or narrative search techniques (legal and Twitter the former, grey literature the latter). In broad terms, a systematic search involves setting clear inclusion and exclusion criteria (e.g. time frame to be searched). The search terms and the databases to consult are decided upon in advance. The search terms are key; they ensure that only relevant evidence will be found. The databases are those that provide quality results (e.g. official governmental sources, legal databases etc.).

This is in contrast to a narrative search, which in broad terms differs from a systematic search in that it sets to capture anecdotal evidence. The investigator chooses websites that are considered appropriate and useful in the context of the research. The search terms are pre-defined, but these can be amended to a more appropriate language common to the website searched. The results are often anecdotal and observational.

Note that we classify the Twitter search as systematic. The resulting evidence was better informed than that generated by the grey literature. This could be accounted for because over 90% of incidents were US based, and thus coming out of an environment used to mandatory data breach reporting. In contrast, UK data breach reporting is not mandatory and potentially not noticed and described by the press in the same way. A further reason could be the demographics of tweeters; using the search terms we did, they appeared to produce hits from a well-informed public.

Stage Two comprised three sets of thematic analyses (also undertaken in parallel), where we categorised harm types, causes and harm/impacts into typologies.

In Stage Three, the typological evidence was merged, so that harms (hard and Twitter evidence) and impact (soft evidence) could be examined in the contexts in which they occurred (i.e. regulatory and social).

Figure 1: Searches for the three evidence strands

Stage One					
	Search One		**Search Two**		**Search Three**
	Hard evidence		Soft evidence		Social Media
Typical sources	UK Case Law; ICO		Newspapers; charities		Twitter
Search type	Systematic search		Narrative search		Systematic search
Stage Two					
	Thematic analysis One		**Thematic analysis Two**		**Thematic analysis Three**
	⇩ Emergent typography		⇩ Emergent typography		⇩ Emergent typography
Stage Three					
⇩ Merged evidence					

1.D Limitations

Our approach has drawn upon evidence ranging from 'hard' sources (such as court rulings, tribunal judgments, enforcement notices and monetary penalties) and social media (Twitter) to 'soft' sources (newspaper articles, charities' and citizens' voice groups' websites). Given time limitations and the breadth of this review, this scoping exercise (as opposed to a systematic literature review) produced a sound reference base dating from the enactment of relevant data protection legislation (the Data Protection Directive 95/46/EC in 1995 and the DPA 1998).

There were five major limitations in this methodology:

1. The brief was to examine the evidence from the standpoint of the UK facing outwards, and this was realistic given the time restraints. As such, the search was a scoping exercise and does not claim to be exhaustive. In real terms, there are other UK-based sources that we did not consult, and other evidence from the EU and beyond are not pursued in great detail in our hard and soft searches. However, the Twitter evidence did produce a preliminary body of US-based evidence.

   1.A With a longer time frame and a more narrowly defined focus, a search for hard evidence could have included the enforcement actions of other European data protection authorities, especially those that have strong histories of data protection jurisprudence, namely Germany and the Nordic countries. As such, more in-depth evidence from the EU and internationally could have been produced. It is likely that cases would have been identified where practice is poorer than, and better than, in the UK.

2. With regard to the soft evidence search, the newspapers listed in Table 2 were searched, but these newspapers only. In real terms and again due to the time restrictions for the review, this excluded any evidence that could be found in other newspapers, or in trade magazines or in peer-reviewed journals.

   2.A It was challenging to pursue the soft evidence strand, due to the nature of the sites investigated. Firstly, it was not possible to use Boolean operators on every site. Secondly, a common term such as 'data breach' was sometimes alien to the language used (e.g. newspapers: the tabloids). To counteract this, we used the same multiple terms for each source (see Table 5).

3. As described under *Research Design*, it was the use of thematic analysis that allowed us to compare findings between and within the three evidence strands. As will become apparent later, the categories we devised were sometimes quite specific (particularly so in the hard evidence strand), but sometimes quite broad. A case in point is the category 'maladministration'. Particularly in the soft evidence strand, there was insufficient evidence to break incidents around maladministration down further (e.g. failure to consider the risks or potential problems, failure to develop suitable systems and procedures). Simultaneously, if we had employed further sub-categories, then many cells in the typology tables (e.g. Table 14) would have been empty. This would have implications for the inferences we could make.

4. The review sought to cross-verify findings by adopting a merged evidence approach. Marrying the hard and soft evidence with good conscience meant that we identified fewer matches than was probably the case. On the one hand, we often had clear statements of fact and process (hard evidence) and on the other, non-regulatory language open to interpretation (soft evidence). At the same time we gathered Twitter evidence, which regularly referred to more traditional media websites, trade magazines etc. This limitation also goes some way to explain why certain categories were very broad when generating the typologies.

5. After initial searches it became apparent that searching for 'harm' (or, indeed, 'abuse') would not lead us to the evidence. Rather, we had to extend our search, and seek out 'harm' through 'proxy' search terms such as 'data breach' but also employ wider more generic searches for anything involving the terms health, medical, biomedical or genetic data.[7]

[7] Further details on search terms used are provided in Section 6.A Hard evidence *Method* below.

1.D.1 Care.data

In our proposal, we had intended to consider care.data and its implications for this review. Since undertaking the review, concerns were raised particularly around the selling of health data to commercial bodies, so much so that the scheme has been postponed and will be subject to further consultation. Due to this suspension of activity, we could not conduct a more meaningful survey of the incidence of harms arising out of the care.data scheme or the resultant implications for governance. However, we do note that the suspension of care.data was in response to strong public outcry – but not because of evidence of harm as such. This having been said, the passing of individually identifiable data to actuaries by the previous data custodians, might indeed have been perceived as some as a form of 'harm'. Care.data is a salutary lesson in the need for robust and timely public engagement – as opposed to mere communication – and in understanding the range of ways in which data subjects might perceive harms arising from uses of their data.

1.D.2 Limitations inherent to the judicial and regulatory system

As the DPA falls within the remit of both civil and criminal jurisdiction,[8] it is important to highlight the relatively ***few*** cases overall that goes to trial and thus these few cases only would be found within the hard evidence review. Between January and March 2014, whilst there were over 424,500 new claims filed in civil courts in England and Wales, only 11,800 trials or hearings were held and importantly, only 3.0% to 3.5% of civil claims (historically) go to trial.[9] Furthermore, of the 96.5% to 97% of trials that do *not* go to trial, the settlements could be subject to stringent confidentiality agreements further restricting the flow of information.[10] Criminal offences under the DPA may only be brought forward by the Director of Public Prosecutions and the Information Commissioner in England and Wales[11] - whereby such responsibility lies with the Crown in Scotland and the Director of Public Prosecutions for Northern Ireland in Northern Ireland – which again necessarily narrows the amount of evidence to be found. Given that 'there is no stand-alone offence of failure to comply with the data

[8] Criminal offences under s 21(1), 21(2), 47(1), 55, or 56 of the DPA.
[9] Ministry of Justice, 'Court Statistics (Quarterly) January to March 2014', 19 June 2014 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/321352/court-statistics-jan-mar-2014.pdf> accessed 19 June 2014.
[10] Although the use of 'gagging' clauses in the NHS were banned in 2013 in England and Wales, as well as in Scotland, previous use of gagging clauses may have impacted the number of cases brought forward by former staff of various NHS Trusts. This will have influenced the flow (lack thereof) of information regarding poor patient care practices and standards; information that may have been used in court by affected patients and/or their families. The 2014 House of Commons Library Standard Note 'Whistleblowing and gagging clauses: the Public Interest Disclosure Act 1998' considered the use of gagging clauses in the NHS to silence whistle-blowers and the subsequent ban of gagging clauses in 2013. <www.parliament.uk/briefing-papers/sn00248.pdf> accessed 19 June 2014. See also: House of Commons Committee of Public Accounts 'Confidentiality Clauses and Special Severance Payments' (June 2014) <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmpubacc/477/477.pdf> 19 June 2014; and on Scotland's banning of confidentiality clauses in NHS Scotland settlement agreements, 'Confidentiality clauses' (*Scottish Government*, 2014) <http://news.scotland.gov.uk/News/Confidentiality-clauses-9d2.aspx> accessed 19 June 2014.
[11] DPA, s 60.

protection principles',[12] the amount of harm that may go unchecked is potentially quite high.

Within this context, it should also be recognised that each year the ICO receives 'tens of thousands of enquiries, written concerns and complaints about information rights issues,'[13] of which only the most serious will warrant enforcement action of the type that would be publicly reported (e.g. decision notices and monetary penalty notices). Thus, the evidence from the ICO is far from representative of the whole spectrum of harms experienced by individuals. When the ICO provides 'advice and instruction to help ensure the organisation gets it right in future'[14] in response to a complaint received, this will unlikely be made public unless or until more serious or persistent contraventions of the DPA occur in relation to that original complaint. Whilst in the more serious and limited number of cases where the ICO imposes a monetary penalty of up to £500,000 or for criminal breaches of the DPA where individuals or organisations are prosecuted, such enforcement actions *are* publicised on the ICO website.

[12] Gillian Black, 'Data Protection Re-issue', para 324.
[13] ICO, 'Handling concerns and complaints' <http://ico.org.uk/what_we_cover/handling_complaints> accessed 25 April 2014.
[14] ICO, 'Handling concerns and complaints'.

2. Introduction

2.A Context of the evidence review

In this digital age of growing interconnectivity and digital advances, there are now opportunities in place that are exceptionally beneficial to world citizens in terms of information, communication and improvements to quality of life. Medical advances, clinical interventions, and access to these are progressing at great speed; indeed, personalised medicine is now on the horizon. Particularly in the biomedical and healthcare settings, there is on the one hand a knowledge base that can and, many would argue, should be shared. On the other hand, there is the individual whose sensitive personal data must be treated with appropriate respect and care. An array of regulations are in place to facilitate the twin aims of both promoting data sharing in the individual and public interests, and of protecting the core privacy interests that are at stake.

In this context, it is important to consider the prevalence of data breaches *across* sectors as it illuminates the broader landscape within which the abuse of health and biomedical data is located. Therefore we briefly consider breach rates both within the UK health sector and between sectors. Firstly we present the figures on breach rates between sectors in the UK. In its recent publication, the ICO presented its figures for the three quarters April to December 2013. A total of 43 sectors are listed, and for the sake of brevity we report here only a selection of these for comparison purposes. In Table 3 we have calculated the percentage of breaches by sector based on the total number of breaches in all sectors, that is, 406 breaches. Approximately four out of ten breaches occur in the health sector.

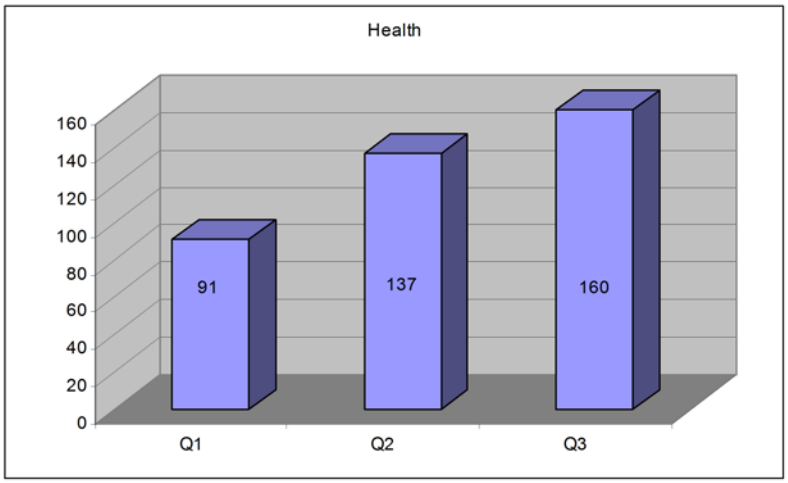
Table 3: Number of breaches in Q3 2013 by sector

Sector	Number	%
Health	160	38.1%
Local Gov	55	13.1%
Education	36	8.6%
Solicitors/Barristers	17	4.0%
Police & Crim records	15	3.6%
Housing	14	3.3%
Cent Gov	13	3.1%
Charities	10	2.4%
Insurance	8	1.9%
Lenders	6	1.4%
Social services	6	1.4%
Financial Advisors	5	1.2%
Courts/Justice	2	0.5%
Debt Collectors	2	0.5%
Pensions	1	0.2%

Probation	1	0.2%
Regulators	1	0.2%
Prisons	0	0.0%

Turning to trends within the health sector, Figure 2 shows an increase of breaches by 23 between Q2 and Q3 and 60 between Q1 and Q3.[15] This trend is clearly of concern, so much so that the ICO conducted an audit on the health sector from August 2012 to January 2014, however in England only.[16]

Figure 2: Health sector – Q1 to Q3 trends in 2013



As the ICO reported, it was encouraged by some improvements to the Information Governance Toolkit (then Version 11, Version 12 now live).[17] However and realistically, in the audit of 19 sites (NHS Trusts, Health Boards, Health & Social Care Trusts and companies with a focus on health services) only one was rated with 'high assurance' (5.2%), nine with 'reasonable assurance' (47.3%), eight with 'limited assurance (42.3%), and indeed one with 'very limited assurance' (5.2%). From this very small England-only sample, we can ascertain that just over half operate under conditions that comply with the Data Protection Act 1998 with high or reasonable assurance, and just under half with limited or very limited assurance.

The results of this audit emphasise that, given the complex nature of hardware, software, end-to-end connectivity protocols, administrative procedures, human error, social engineering and the interactions between these, facilitating appropriate use of sensitive personal data, while delivering suitable levels of technical security and thus privacy can be challenging. Breaches do occur, and these can be harmful in a range of ways to those affected. Although such breaches are being recorded with increasing rigor in the UK (as briefly discussed above), very little is

[15] ICO, 'Trends' <http://ico.org.uk/enforcement/trends> accessed 21 June 2014.
[16] ICO, 'Good Practice. Audit of outcomes analysis: Health – August 2012 to January 2014' <http://ico.org.uk/~/media/documents/library/Data_Protection/Research_and_reports/outcomes_report_health.pdf> accessed 21 June 2014.
[17] 'IG Toolkit Version 12 is Now Live' (2014) <https://www.igt.hscic.gov.uk/whatsnew.aspx> accessed 25 June 2014.

known about the nature and scope of the actual resultant harms to the individual(s) whose interests have been breached, or, indeed, of wider public or societal harms that might occur.

The brief for this report, a scoping exercise, was to provide a review of evidence relating to harm resulting from security breaches or infringements of privacy involving sensitive personal biomedical and health data, as well a search for any evidence of opportunity costs from reluctance or failure to link, share or use data. A major focus was to identify the effect of resultant harms on the data subject. Thus, this review provides:

(a) An examination of the relevant definitions of health and biomedical data, and harm in the regulatory and social context.
(b) The identification of 'actual harms' in the evidence gathered and their prevalence, primarily in the UK context.
(c) A categorisation of the types of uses that resulted in harm and the underlying causes.
(d) An evaluation of the relative effectiveness of governance, sanctions and remedies identified in the evidence.
(e) The consideration of the implications from the evidence within the broader social and legal context.
(f) An overview of areas where future research would be beneficial.

The review was taken from a multi-disciplinary approach, drawing upon the disciplines of law, information governance, data linkage security and social psychology. The multi-disciplinary approach taken adds value in the three-strand approach towards evidence gathering: the 'hard' evidence strand considered hard sources such as court rulings, tribunal judgments and ICO enforcement mechanisms; the 'soft' evidence strand considered soft sources such as newspapers; and the third strand looked to Twitter (with further detail on the approach taken in Section 1 above). The important value added by this three-strand approach offers a broader perspective on the types of harm resulting from uses of health or biomedical data, outwith the regulatory constraints of court cases and administrative enforcement actions. The soft evidence strand in particular, allowed for consideration of comparable incidence of abuse of health and biomedical data in the UK (newspapers) and in an international context (Twitter: mainly the EU and US).

Thus, the remainder of the report follows the broad outline:

a) In ***Section 3 'Definitions'*** we review the relevant regulatory definitions for health and biomedical data that determines the initial scope of the evidence review, along with definitions of 'harm' according to data protection law, in comparison to 'harm' in a psycho-social context.
b) In **Section 4 'Abuse and harm – categories, causes and impact'** we provide the categories of abuse, causes and spectrums of harm/impact that encompass this review.

c) The content of ***Section 5 'Methodology/Approach'*** has been moved to Section 1.A Background to the evidence review. We keep Section 5 in as a placeholder, so that the social scientist reader will be directed to Section 1.

d) In ***Section 6 'Method'*** the search criteria and the constraints encountered for each strand are explained.

e) In ***Section 7 'Results'*** the results are presented in three stages: (i) initial findings, (ii) emergent typologies, and (iii) merged evidence.

f) In ***Section 8 'Conclusions'*** we infer initial conclusions from our findings.

g) In ***Section 9 'Implications'*** we look at the implications of our findings for governance and those who must work with and within them, whilst considering the presence of incentives and disincentives to abuse. Section 8 also evaluates the efficacy of the sanctions and remedies identified in the evidence.

h) In ***Section 10, 'Future Research'***, we identify areas that would warrant further research.

2.B Research questions and pathways to answers

As made apparent in this section, this was an expansive remit. Here we reiterate the purposes and scope of the Brief for Tender insofar as it relates to the questions we posed at the literature search stage. The purpose of the evidence review included:

> 'Assisting the commissioning parties to understand:
>
> The nature of the actual harms resulting from data misuse or security breaches involving sensitive personal biomedical and health data.
>
> How the incidence and prevalence of such harms is assessed, inherent limitations to methodologies of assessment, and the appropriate context in which to assess them'.[18]

The scope of the review in the Brief for Tender noted that:

> 'The harms that are relevant may … be things such as:
>
> - discriminatory treatment (whether unlawful or not), for example instances of 'genetic discrimination';
> - stigmatisation, reputational damage either of individuals or of groups with particular characteristics (e.g., linking socio-demographic information with health indicators);
> - psychological harm due to loss of privacy;
> - loss or damage to property (including intellectual property) or income (e.g. from 'identity theft');
> - reputational damage and loss of public trust in research or healthcare resulting from misuses of data or privacy breaches;

[18] Taken from the 'Evidence Review: brief for tender' 1-2.

- missed opportunities from reluctance or failure to link, share or use data (e.g. failure to identify abuse, improve services or advance scientific knowledge) …'[19]

Further it was requested that evidence should be sought in sources such as:

- '… published reports (e.g. ICO/ Information Tribunal proceedings, media reports) … and
- relevant documented cases of harm, including grey literature and other non-academic sources.' [20]

Therefore in our search, we sought to gather evidence to answer the following questions:

1. **Where do we find evidence of missed opportunities from reluctance or failure to link, share or use data and what are the prevalence rates?**

2. **Where do we find evidence of discriminatory treatment or stigmatisation and reputational damage (to individuals or to groups) and what are the prevalence rates?**

3. **Where do we find evidence of psychological harm (due to loss of privacy or otherwise) and what are the prevalence rates?**

4. **Where do we find evidence of damage to property or income and what are the prevalence rates?**

These central questions guided our choice of media to be consulted. The hard evidence strand, encompassing legal decisions or enforcement actions, related to the abuse of health or biomedical data, and would enable us to discern how robust governance and enforcement measures currently operate in the UK. This strand would also allow us to understand how 'harm' in this context is *officially* or legally recognised. This required an important contrast, encapsulated by the soft evidence strand, which could present evidence without the same regulatory constraints. Most importantly, the soft evidence could offer evidence of harm firstly that might otherwise not be legally recognised (or thus remedied) and secondly bring in anecdotal evidence from the data subjects, including impact statements regarding the harm. Finally, the Twitter strand of the evidence review would provide a final 'check' for evidence not caught through either official, legal channels or traditional media (e.g. newspapers).

[19] Taken from the 'Evidence Review: brief for tender' 2-3.
[20] Taken from the 'Evidence Review: brief for tender' 3.

3. Definitions and Initial Classifications of Abuse, Cause for Abuse and Harm

3.A The regulation of health and biomedical data

To understand the potential harms that might arise out of the abuse of health or biomedical data, the context in which harms are measured and sanctioned must be considered. The regulatory landscape that governs the processing of personal data in the UK is the relevant context for the hard evidence scoping exercise. The regulatory context is particular to the 'hard' evidence strand, because harm will be legally recognised only where there is a concomitant breach of the relevant laws – in this case, the UK's Data Protection Act 1998 (DPA)[21], breach of the common law duty of confidentiality, and breaches of the European Convention on Human Rights (in particular Article 8's right to respect of private and family life). A chief aim of the DPA is to promote good data protection practice, whilst ultimately serving a regulatory function for data processing in the UK.[22] As such, the DPA is particularly relevant for this evidence review given the structure it lends to more contextual inquiries associated with particular *types* of data and the concomitant obligations that attach to more 'sensitive' types including health and biomedical data.

As the DPA represents the UK's implementation of the Data Protection Directive 95/46/EC (DPD), the dual aims of the DPD must be taken into account – facilitating data processing (for the maintenance of internal market) whilst protecting individuals' fundamental rights and freedoms (reflective of the regulatory function).[23] This dual-purpose lends to another aspect of this evidence review which namely seeks evidence of harm arising from *non*-use of health or biomedical data – the aim of data protection law to ensure the free flow of personal data, whilst protecting and promoting individual privacy, reflects the notion that failure to use personal data can also be harmful to individuals and/or broader public interests.

As such, we are concerned with situations where data controllers' data handling practices fall below the standards set forth by the DPA and are thus fined by the ICO, but also where failure to use health or biomedical data causes suboptimal use of data from the point of view of the development of scientific knowledge, securing health outcomes, promoting economic growth

[21] Data Protection Act 1998. (DPA)
[22] DPA, Introductory Text;
[23] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ 281 Recitals 1-3 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> accessed 17 June 2014. (DPD)

and wider public benefits etc. It is within this context of regulation that *hard* evidence of harm must be viewed. However and importantly, the hard evidence of harm must be contrasted with the soft evidence of harm, whereby the latter includes justifiably wider conceptions of harm that are not necessarily recognised or provided for under the existing legal framework.

3.A.1 Personal and sensitive personal data under the DPA

To understand the *scope* of this review, it is important to consider and adopt a working definition of health and biomedical data, as per the Brief for this report. Under the DPA, data are categorised according to the sensitivity associated with the data in question. In the context of this report, the DPA will apply where the health or biomedical data in question meet the initial threshold: that the data are personal or sensitive personal data. ***Personal data*** are:

Data, which relate to a living individual who can be identified from those data, or from those data and other information, which is in the possession of, or is likely to come into the possession of, the data controller. [24]

The DPA enumerates specific categories of sensitive personal data that are considered to carry more risk to individual privacy and other personal interests. Only *health* data of an individual are considered ***sensitive personal data*** under the DPA and thus enjoy greater procedural safeguards when processed.[25] Whilst *health* data are specifically enumerated as a category of sensitive personal data, *biomedical* data, which encompass a wider range of health-related data, are not so distinguished. Likewise, *genetic* data are not enumerated as a category of sensitive personal data under the DPA.

However, in looking to the potential future regulation of data in the UK, a previous draft of the European Commission's proposed Data Protection Regulation (pDPR)[26] considered biomedical data as a *subset* of health data including 'the actual physiological or biomedical state of the data subject independent of its source, such as for example from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.'[27] Genetic data are treated as an entirely *separate* category, defined as '…all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal

[24] And thus are not 'anonymous' data. DPA, s1(1).
[25] The processing of sensitive personal data requires additional lawful justification under the DPA. DPA, s2; ICO, 'Key definitions of the Data Protection Act'. <http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions> accessed 24 February 2014.
[26] If enacted, the pDPR would have direct effect in the UK, as a regulation does not require national legislation to implement it, like with the current Data Protection Directive 95/46/EC and thus the UK's DPA 1998. European Commission, 'Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM (2012) 11 <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf > accessed 6 April 2014. (pDPR)
[27] This definition is from the original draft pDPR, published in January 2012, Recital 26: <http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf > accessed 11 June 2014.

development'.[28] Importantly, both genetic data and health data (the latter encompassing biomedical data) were treated as 'special' or sensitive categories of personal data.[29]

The most recent draft of the pDPR reverts to a definition similar to that which is currently under the DPA for health data (i.e. '*any* personal data which relates to the physical or mental health of an individual, or to the provision of health services to the individual').[30] Given that this definition of health data refers to *any* personal data concerning health that relates to the physical or mental health of an individual or to the provision of health services to the individual, it is reasonable to assume this is broad enough to encapsulate *biomedical* data. Biomedical data refer to the 'actual physiological or biomedical state of the data subject', as an extension of data relating to physical health.[31] The definition of *genetic* data is expanded in this most recent draft, but remains categorised as a *separate* category of 'special' or *sensitive* personal data.

Overall, the addition of biomedical and genetic considerations to the regulation of processing special or sensitive types of personal data is welcome. This demonstrates an acknowledgement of the technological advancements made – in medicine, research and information technology – since the enactment of the DPD and thus DPA in the UK. Importantly, by categorising health, biomedical and genetic data as 'special' and thus imposing further regulatory safeguards when processing such data, it recognises the greater risks involved if health, biomedical or genetic data are abused. The proposed regulatory definitions are in line with the Brief for this report, which focuses on health and biomedical data as particularly sensitive categories of data. Therefore we adopt and employ the terms given in the Brief for Tender for this report, **health and biomedical data**, to mean in the broadest sense:

Health and biomedical data:

Any personal data that relate to the physical or mental health of an individual, or to the provision of health services to the individual. This includes biomedical data, gathered from any source (e.g. from blood samples, in vitro diagnostic tests) that speaks to the actual physiological or biomedical state of the individual.

[32]

[28] pDPR (January 2012), Article 4(10).
[29] pDPR (January 2012), Article 9(1).
[30] pDPR (as agreed by European Parliament on 14 March 2014), Art 4(12) (2014) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN> accessed 11 June 2014. (emphasis added)
[31] Whereas the DPA is not so inclusive and rather only stipulates that sensitive personal data include that which speaks to 'his physical or mental health or condition'. Arguably, the inclusion of the word 'any' in the most recent draft of the pDPR offers a much broader allowance for what can be considered health data.
[32] Genetic data are traditionally considered as a separate category of sensitive personal data, as it was, for example, treated separately from health and biomedical data in the pDPR and in relevant literature such as: Graeme Laurie, *Genetic privacy: a challenge to medico-legal norms* (Cambridge University Press 2002); Mark Taylor, *Genetic Data and the Law: a critical perspective on privacy protection*

It is important to distinguish between the *information* derived from a physical sample that can speak to an individual's actual physiological or biomedical state as opposed to the ***material*** itself,[33] which would be governed by laws relating to human tissues and samples, for example the Human Tissue Act 2004.[34]

We now turn to other regulatory definitions that will help to define the scope of this evidence review as well as enhance the understanding of where harm may or may not be legally found or thus officially recognised.

3.A.2 Identifiability and de-identification of data

The ***identifiability*** of an individual from data is a threshold concept for determining whether the data in question are *personal* data, and thus whether data protection law applies. However, identifiability of data may also relates to the propensity for the abuse of personal data to cause harm – arguably, the more identifiable data are, the greater the chances for causing harm in the ways considered in this report.[35] It is identifiable data (rather than anonymised data) that could be abused in a way that causes actual harm to individuals such as through discriminatory treatment or psychological harm due to the loss of privacy – however we recognise that masking identifiability may only prevent or protect human interests particular to identification and privacy. Nonetheless, the identifiability of data bridges an important, conceptual gap between the nature of data and the potential risk of harm:

Data are *identifiable* if:

The data present a risk of identification that is greater than a remote possibility whether by direct (identification from a single source) or indirect means (identification from a combination of sources).

(Cambridge University Press 2012). We identify genetic data as an area warranting a focused piece of future research – see 10.D Future research on genetic data.

[33] Similarly, and in regards to genetic data versus genetic *information*, see: Mark Taylor, *Genetic data and the law : a critical perspective on privacy protection* (Cambridge University Press 2012).

[34] Given space constraints and this report's focus on health and biomedical *data*, we will not investigate the regulatory complexities that arise when dealing with human *materials* (tissues) and the associated personal data held together. However key legislation and literature include: Human Tissue Act 2004 (HTA 2004); Graeme Laurie, Kathryn Hunter, and Sarah Cunningham-Burley, 'Guthrie Cards in Scotland: Ethical, Legal and Social Issues' (The Scottish Government 2013); Graeme Laurie and Shawn Harmon, 'Through the Thicket and Across the Divide: Successfully Navigating the Regulatory Landscape in Life Sciences Research' (2013).

[35] Whereas the identifiability of an individual from data is a threshold concept for application of the DPA, the identifiability of data as it relates to *a propensity to cause abuse and thus harm to individuals* is **commentary** derived from **interpretation** of the law as it relates to the context of this report. The focus on *identifiability* as a core (or chief) aim of privacy protection is considered in our discussion of the *Source Informatics* case(UKC14) in Section 8.A.4 *Harm outwith privacy harms*. Here we contend that good governance may require accounting for a fuller range of human interests – those that are implicated in the processing of health and biomedical data, including dignity, autonomy and identity.

De-identification, which includes methods for anonymising data, 'is an effective way to protect the privacy of patients when their data are used or disclosed',[36] and thus enables data controllers to minimise the risk of harm to individuals. As the definition of identifiability above suggests, the key to *effective* de-identification lies in a distinction between *identifiable* data (which are fairly, or reliably identifiable) and data which have minimal risk of identification (or perhaps no reliable means of re-identification). What is potentially problematic is the case where data might *possibly* be re-identified (at least in some instances) – and then whether such data can be considered sufficiently de-identified or thus used safely without increased risk to individuals' privacy. It is especially important to distinguish where there is risk in (re)identifying a *single* record versus an entire data set, whereby the risks are higher if the identifiability of a single record can identify the whole set (making all data, therefore, personal data).

Key literature within the area of *de-identification* considers the risk to individual privacy (or thus the risk of harm to individuals) in terms of access to and the identifiability of individuals from the data, whereby the more restricted the access and more de-identified the data, the less risk is posed to individual privacy.[37] Equally, there is growing literature to suggest that complete reduction of this risk – in terms of eliminating all chances of re-identification – is increasingly difficult, or indeed impossible.[38] Within the specific context of processing health or biomedical data, the ability for data controllers to sufficiently de-identify or anonymise data is paramount. 'Sufficiently', In terms of de-identification, 'sufficiently' means reaching a point where the data controllers are satisfied that 'the data does not…identify any individual and [are] unlikely to allow any individual to be identified through…combination with other data'.[39] Thus, there is minimal risk of identification (or without a reliable means of doing so).

De-identification proves key to minimising the risk of harm to individuals, but also can minimise regulatory burden (as the DPA does not apply to *anonymised* data). If data are *anonymous,* there is a much narrower scope for finding 'breaches' of the relevant law. Indeed, if the data are 'adequately' anonymised the DPA does not apply at all, but the devil is in the detail of what actions must be taken and maintained to secure this level of de-identification.

[36] Khaled El Emam, *Guide to the De-Identification of Personal Health Information* (CRC Press Taylor & Francis Group 2013) 2.

[37] El Emam, *Guide to the De-Identification of Personal Health Information* 4.

[38] For example: Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 UCLA Law Review 1701–1777 on the fallacy that is anonymisation. Well known re-identification attacks also highlight this issue: Michael Barbaro and Tom Zeller, 'A Face Is Exposed for AOL Searcher No. 4417749 - New York Times', no date; Ryan Singel, 'Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims | Threat Level', December 17, 2009 <http://www.wired.com/2009/12/netflix-privacy-lawsuit/> accessed 29 April 2014.

[39] The Information Commissioner's Office, 'Anonymisation: managing data protection risk code of practice', November 20, 2012 6.

Pseudonymous data (defined by the ICO as data that distinguish individuals in a dataset by using a unique identifier, but that does not reveal their 'real world' identity[40]) is a form of de-identification that is considered to be at the higher-risk end of the anonymisation spectrum.[41] Neither the DPA nor the Data Protection Directive 95/46[42] (DPD) provides a definition for pseudonymous data. The ICO considers pseudonymisation as posing a higher privacy risk given its production of *individual*-level records.[43] This higher privacy risk entails a higher risk for potential harm to arise from the use or abuse of pseudonymised health or biomedical data, more so than if more stringent technical anonymisation standards have been used (e.g. where anonymised records are provided at population-level rather than individual-level).[44] However, and importantly, pseudonymous data is (under current interpretations by the ICO) capable of being 'anonymous' and thus outwith the scope of the DPA.[45]

The pDPR has implications for the concept of identifiability; first in regards to whether the regulatory regime applies to particular data, and second in how harm is recognised within the law. The current draft of the pDPR *lowers* the threshold for identifiability by defining pseudonymous data as a specific *subset* of personal data.[46] Under current interpretations of the DPA, pseudonymous data would theoretically only be treated as *personal data* if, for instance, the data controller held the 'key' or unique identifier that could re-identify the data set, or in other words the data were capable of re-identifying individuals' real world identity.[47] However and importantly, the current draft of the pDPR ***automatically*** categorises pseudonymous data as personal data ***regardless*** of whether the data controller in question has the ability to re-identify the data subject(s) – the singling out of an individual by means of a unique identifier is enough. This is a clear step above the status quo where this determination is made only after consideration of the particular circumstances of each case (e.g. such as when a "Trusted third

[40] The Information Commissioner's Office, 'Anonymisation: managing data protection risk code of practice' 49.

[41] The ICO considers pseudonymisation as higher risk than other forms of anonymisation 'because even though pseudonymised data does not identify an individual, in the hands of those who do not have access to the 'key', the possibility of linking several anonymised datasets to the same individual can be a precursor to identification.' The Information Commissioner's Office, 'Anonymisation: managing data protection risk code of practice' (2012) 21. <http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf> accessed 12 June 2014. (Hereinafter, 'Anonymisation Code of Practice')

[42] 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data'. (DPD)

[43] ICO, 'Anonymisation Code of Practice' 7.

[44] For example, if the health or biomedical data in question were anonymised to only allow aggregate or population level analysis, with no individual records produced.

[45] Whereby the ICO considers that pseudonymisation '…can present a greater privacy risk, but not necessarily an insurmountable one.' ICO, Anonymisation Code of Practice 7.

[46] Pseudonymous data is defined as 'personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution.' pDPR, Art 4(2)(a) (2014).

[47] In the ICO's 'Anonymisation Code of Practice' the likelihood of pseudonymous data being re-identified is directly related to the access (or potential access) to the 'key' to unlocking the otherwise anonymous, individual level records. ICO, 'Anonymisation Code of Practice' 21.

party" is used to link personal data sets on behalf of a data controller, such that the data controller never has the ability to re-identify the data once pseudonymised[48]).[49]

Ultimately, this definition would mean that pseudonymous data would be caught by the data protection regime as would any other form of personal data. The potential effect of this would be a broader capacity of the law to recognise breaches involving pseudonymous data and thus provide remedies to individuals where there currently are none. However, this could have very significant effects on medical and biomedical research.[50]

Overall, the level of identifiability and level of anonymisation applied to data can affect the likelihood that harm may be caused through use or abuse of such data. Therefore, whether data are sufficiently anonymised will remain a key question for data controllers when assessing the level of risk posed by a particular use of data. Given the focus of data protection law on the *informational privacy* of individuals and identifiability, this report begins with a working assumption that any hard evidence uncovered, as representative of breaches under data protection law, would *not* be characterised as harmful to individuals if data were anonymised.[51] This means that use of anonymised data will not be categorised or considered as harmful to individuals, if the data remained anonymised, and individual identity was not revealed or otherwise compromised. However, it is understood that the use or abuse of health or biomedical data can and does affect a wide range of human interests including autonomy, dignity and privacy.[52] The effect of abuse of data on these other human interests will be considered under

[48] An example of a Trusted third party (TTP) service is provided by the Administrative Data Linkage Service (ADLS), which '…provides researchers and data holding organisations a mechanism to enable the combining and enhancing of data for research to which may not have otherwise been possible because of data privacy and security concerns.' In situations where a TTP service is used, it is arguable whether the de-identified data set ultimately transferred to the data controller, and that has no ability to re-identify (as the keys were destroyed by the TTP after transfer), is *personal* data for the purposes of the DPA.

[49] The ICO takes the position that effective anonymisation through pseudonymisation is *not* impossible, if a) pseudonymous are *not* re-identified; or b) if re-identified, none of the data protection principles are breached. This position is contrary to the definition of pseudonymous data in the recent draft of the pDPR, which predetermines all pseudonymous data as a subset of personal data without consideration of probabilities of re-identification or access to the re-identifying keys. ICO, 'Anonymisation Code of Practice' 21.

[50] It is outwith the scope of this report to consider the full implications of the pDPR upon the health and biomedical research sectors; however it is clear that there is concern over how the Regulation would impact (negatively) upon the processing of personal data for health and biomedical purposes. The Wellcome Trust has consistently opposed drafts of the pDPR, which purport to turn pseudonymous data into a subset of personal data that would interfere with publicly beneficial research from being carried out. See: <http://www.wellcome.ac.uk/stellent/groups/corporatesite/@policy_communications/documents/web_document/wtp051900.pdf > accessed 12 June 2014.

[51] Assessing whether data is sufficiently anonymised is largely a technical assessment that is dependent partially on the state of technology, security developments or changes to the public availability of certain records. ICO, 'Determining what is personal data' (2012) 9 <http://ico.org.uk/for_organisations/data_protection/the_guide/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PERSONAL_DATA_FLOWCHART_V1_WITH_PREFACE001.ashx> accessed 24 February 2014.

[52] For specific discussion of the other human interests at stake when abuse of data, and prospect of harm despite the use of anonymous data see: Deryck Beyleveld and Elise Histed, 'Betrayal of confidence in the Court of Appeal' (2000) 4 Medical Law International 277–311.

3.C below when the broader conception of harm is discussed in context of the soft evidence strand of this review.

3.B Harm under data protection law – harm as damage or distress

Given that the 'hard evidence' strand of this report is focused on uncovering evidence of harm relating to health or biomedical *data* within the context of breaches of relevant *law*, it is vital to understand how harm is recognised or compensated for under data protection legislation. Harm caused to individuals arising out of contraventions of the DPA is framed narrowly within the Act, having the effect that an individual might suffer harm but not to a *sufficient* degree to constitute a breach or warrant a remedy under the law. Under the DPA harm is recognised in terms of **damage** and **distress** – damage as financial harm and distress as emotional harm. For the purposes of this review, the relevant courses of action that an individual can refer to if they suffer damage or distress (or will be *likely* to suffer *unwarranted, substantial* damage or distress) arising out of processing their personal data include:

- Preventing the processing of their personal data;[53]
- Seeking the rectification, blocking, erasure and/or destruction of their personal data;[54] and/or
- Receiving compensation for a data controller's contravention of the DPA as it affects their personal data.[55]

The limited scope of redress available to individuals for 'harms' arising out of contraventions of the DPA highlight the narrow context within which the hard evidence strand operates. Taking each of the above actions in turn, the limits to the regulatory notions of harm and related (in)capacity to compensate adequately are considered.

3.B.1 Preventative measures of redress under the DPA

Under the DPA section 10, individuals have the power to *prevent* instances of harm if they feel *subjectively* that the processing of their personal data for a specified purpose or in a specified manner is a) causing or is likely to cause substantial damage or substantial distress to them or another ***and*** b) that the damage or distress is or would be unwarranted. Whilst section 10 provides individuals with the possibility of preventing harmful processing for himself/herself (or someone else), this right of action is severely limited. Firstly, an individual ***cannot*** prevent such processing if a data controller has satisfied any of the first conditions to processing under Schedule 2 of the DPA, or if the processing meets any similar conditions as set forth by an

[53] DPA, s 10.
[54] DPA, s 14.
[55] DPA, s 13.

order of the Secretary of State.[56] Secondly, even if the individual can prevent processing, a data controller may simply reply within the requisite 21-day period, stating his or her reasons for finding the request unjustified and thus their reasons for not complying with the request.[57] Thirdly, if the processing has begun because the request was refused and/or is continuing, there is no recourse for the individual but through court order, which may be prohibitive in terms of time, costs etc.[58] Fourthly and finally, an individual's request to prevent processing must meet an extremely high threshold – the damage or distress must be both *substantial* and *unwarranted* (neither of which are defined in the DPA).

While unwarranted and substantial damage or distress are not defined in the DPA, the ICO's guidance provides that substantial *damage* must result in physical or financial harm, whilst substantial *distress* must affect an individual to a point beyond '…annoyance or irritation, strong dislike, or a feeling that the processing is morally abhorrent.'[59] This already narrow conception of harm is further constrained by the fact that the substantial damage or distress must also be *unwarranted* – this allows for the caveat that data controllers might have legally justifiable reasons for holding and processing data, including circumstances that might cast individuals in a negative light.[60] Therefore, even if harm is found to be *substantial,* it is possible under the DPA that this might be justified under the circumstances. This reiterates the point above, that a person might *in fact* suffer harm but not have remedies under the law if harm is not of a sufficient degree. These factors will necessarily limit any potential evidence to be found in cases where individuals may have simply given up in their attempts to prevent harmful processing of their health or biomedical data.

3.B.2 Seeking redress *post*-harm under the DPA

Individuals may also seek redress *after* harmful processing of their personal data has occurred. These actions of redress can be divided in terms of compensatory and non-compensatory redress.

3.B.2.A Non-compensatory redress under the DPA

Considering *non*-compensatory redress, an individual may apply to a court to have his/her personal data rectified, blocked, erased or destroyed if inaccurate. An individual may also have their data rectified, blocked, erased or destroyed if a) they have suffered financial damage due to a contravention of the DPA by the data controller; b) they are entitled to receive

[56] For instance, if the processing of personal data in question is 1) legally justified on the basis of the individual's consent; 2) necessary to perform a contract the individual is party to, or is seeking to be party to; 3) necessary to satisfy a data controller's legal obligations; or 4) necessary to protect the vital interests of the individual, s 10 does *not* apply and the individual cannot prevent the processing. DPA, s 10(2).
[57] DPA, s 10(3).
[58] DPA, s 10(4).
[59] ICO, 'Preventing processing likely to cause damage or distress' <http://ico.org.uk/for_organisations/data_protection/the_guide/principle_6/damage_or_distress> accessed 24 February 2014.
[60] ICO, 'Preventing processing likely to cause damage or distress'.

compensation (and thus meet the requirements) under section 13; and c) there is substantial risk of further contravention of the DPA if the data are not so rectified, blocked, erased or destroyed.

Similar to *preventing* the potentially/or actually harmful processing of personal data under section 10 of the DPA, the rights of an individual to rectify, block, erase or destroy records of their personal data are severely qualified and thus limited. First, individuals cannot simply provide written notice to the 'offending' data controller – they may only seek such recourse through the courts system which is prohibitive in terms of times, costs, etc.[61] Second, if the personal data are not *inaccurate* but nevertheless cause an individual continuous distress they are not able to seek rectification, blocking, erasure or destruction of their data. They must meet the extremely high threshold that involves a) proving they suffered *financial* damage as a result of the data controller's breach of the DPA; b) meeting the similarly high threshold for receiving compensation in section 13 (to be discussed further below); and c) proving a 'substantial' risk that the data controller in question will continue to contravene the DPA.[62]

3.B.2.B Compensation under the DPA

Looking to the final possibility for an individual seeking redress under the DPA, as it applies to the context of this report, an individual may seek *compensation* for a data controller's contravention of the DPA if a) it causes the individual (*financial*) damage or b) causes the individual distress, but he or she also suffers damage by reason of the contravention or c) he or she suffers distress and the contravention relates to the processing of personal data for the special purposes (journalism, literature, art).[63] As neither damage nor distress is defined under the DPA, we interpret damage and distress in terms of the ICO's guidance on the parameters of section 13 and the right compensation. Importantly (and similar to section 10 and the right to prevent processing), damage is equated with *financial* loss. The ICO advises in relation to section 13 that 'an individual who has suffered financial loss because of a breach of the Act is likely to be entitled to compensation.'[64]

As to distress, the ICO provides that:

> If an individual has suffered damage, any compensation awarded may take into account the level of any associated distress, but **distress alone will not usually be sufficient to entitle an individual to compensation** (unless the processing was for the purposes of journalism, literature or art).[65]

[61] DPA, s 14(1).
[62] DPA, s 14(4).
[63] DPA, s 13.
[64] ICO, 'Compensation' <http://ico.org.uk/for_organisations/data_protection/the_guide/principle_6/compensation> accessed 13 June 2014.
[65] ICO, 'Compensation'.

Thus and similar to the other forms of redress under the DPA, compensation is severely limited. First, an individual faces similar barriers in seeking compensation; as such, rights are only enforceable through the courts. Second, whilst financial harm is only one of many types of harm an individual might suffer due to a data controllers' abuse of their data, distress itself is non-compensable – the distress must be tied causally to a further financial loss. For example, distress caused by reputational damage is not provided for unless a financial loss can be traced to the loss of professional reputation.[66] Third and most importantly, even if financial loss and distress are proven, the defence for claims to compensation provide a remarkably low threshold to meet – a data controller need only prove they took all reasonable care in the circumstances to avoid the breach in question.[67] As a final note, there are no guidelines as to the level of compensation that might be appropriate – it will depend entirely on the circumstances of each case, to be decided by the courts if the data controller and individual do not come to an agreement.[68] Thus, even where all requirements are met under section 13, there is little precedent in terms of how much compensation individuals can expect to receive. And previous case law indicates that where section 13 requirements are met, damages will unlikely go beyond a nominal amount and/or are awarded on another legal basis. In fact, the recent Court of Appeals case *Halliday v Creation Consumer Finance Ltd* found that the compensation provision under section 13 of the DPA was not intended to produce substantial awards of damages.[69]

However, post *Douglas v Hello!* No 3,[70] a case involving the publication of photos from Michael Douglas and Catherine Zeta Jones' wedding, it appears that courts are *more* willing to compensate for harms arising as a result of *breach of confidence* (and now often understood as misuse of private information[71]); notably for the distress caused by loss of privacy.[72] In *Douglas*, the claimants were awarded £3,750 each for distress, and £7,000 for wasted costs, but only £50 each in compensation under DPA 1998.[73] This ruling is important in context of this report as it shows the narrow limits to which compensation for harm may be awarded under the DPA, whilst under other common law actions (such as breach of confidence or misuse of private

[66] Johnson v Medical Defence Union [2006] EWHC 321 (Ch) at [218] ff, 89 BMLR 43, per Rimer J.
[67] In this regard, the ICO advises that taking 'all reasonable care in the circumstances' would include looking '…at the way you process and protect personal data and that you put in place appropriate checks to prevent any problems occurring. Your defence may rely on describing these checks. Some form of positive action is often necessary and, if a reasonable step or precaution has not been taken, then the defence is likely to fail.' Arguably this is not a high standard to meet. DPA s 13(3).
[68] ICO, 'Compensation'.
[69] *Halliday v Creation Consumer Finance Ltd (CCF)* [2013] EWCA Civ 333 [36].
[70] Douglas v Hello! No 3 [2003] EWHC 786 (Ch).
[71] In *Campbell v MGN Ltd* [2004] 2 AC 457, [2004] 2 All ER 995, the focus in breach of confidence shifted from the need for a pre-existing confidential relationship to focus on the misuse of private information. (Lord Hope)
[72] [2003] EWHC 786 (Ch).
[73] Importantly, the Court determined that the cause for the Douglas's distress was *not* due to contravention of the DPA and thus only awarded nominal damages (£50 each). [2003] EWHC 786 (Ch) para [289].

information) compensation may be wider and thus indicate the law's recognition of a broader conception of harm.

3.B.3 Final thoughts on the legal notion of harm under the DPA

In reviewing the three main types of redress an individual may seek for harms caused by the processing of their personal data, the narrow conception of harm under the DPA, and similarly narrow provisions for compensation/ redress were highlighted.

In summary, harm under the DPA and thus UK regulatory context is understood as:

Harm:

Harm that causes financial damage (loss) to the individual, whereby if distress is suffered, it must a) be beyond mere discomfort – physical, emotional or otherwise and b) to be compensable, be connected causally to a financial loss.

The hard evidence of harm uncovered in the evidence review and specifically those incidents that relate to breaches of the DPA, will take this working definition of harm into account.[74] This definition acknowledges the narrow provision for harm offered by the law in the UK, whilst allowing for contrast between the actual and potential incidents of harm uncovered but that are not necessarily *legally* recognised or compensated for. Importantly, this definition does not reflect the broader conception of harm supported in this report – rather, it reflects the *legal realities* governing use of personal (health and biomedical) data in the UK. As such this narrow, regulatory notion of harm and the related provisions for redress/compensation will be contrasted to the wider definition of harm underpinning the soft evidence strand of this report in Section 3.C *Harm in other contexts*.

3.B.3.1 Harms to the public interest or organisations

As the discussion regarding the legal notion of harm concludes, it is important to highlight that any harmful impact caused through abuse of data to broader, public interests or organisations is simply not provided for in the regulatory context (or at least not explicitly so). This is so, as the application of the DPA is limited to *personal* data that can be found only where data relate to a *living* individual. Thus it excludes entities such as business or third sector organisations. Importantly, this evidence review *does* take into account the possibility for broader public interests and organisations to be harmed from abuse or non-use of health or biomedical data.

[74] This notion of harm is especially relevant to the UK-focused nature of this report and as it applies to the *legal* context. However, wider conceptions of harm are considered and uncovered in the context of the European Convention of Human Rights and specifically the factors accounted for in the ECtHR's judgments.

3.B.3.2 Redressing 'harm' to broader, public interests under the DPA

In considering the lack of recognition or provision for harms to the broader public interest or organisations under the DPA, we will discuss briefly the ICO's ability to issue monetary penalties for serious contraventions of the DPA and the role these penalties play in the regulatory framework relevant to this review.[75]

The ICO has statutory authority[76] under the DPA to issue monetary penalties (which must not exceed £500,000[77]). The ICO issues monetary penalties in a quasi-judicial fashion, effectively applying data protection rules within the law, without judicial intervention, if a data controller has seriously contravened[78] the DPA, and:

1. The contravention was of a kind likely to cause substantial damage or substantial distress, and;
2. The contravention was deliberate or the data controller or person must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it.[79]

In determining whether the contravention is likely to causes 'substantial' damage or distress, the ICO will consider whether the situation is of 'considerable in importance, value, degree, amount or extent'; whether the damage or distress 'is merely perceived or of real substance'; and where the damage or distress is less than considerable, if a large number of people have suffered and thus the totality of damage or distress is nevertheless substantial.[80]

Whilst finding harm (in substantial damage or distress) is required before the ICO imposes a monetary penalty, such penalties do ***not*** serve the purpose of compensating individuals but rather to '…promote compliance with the [DPA]... The possibility of a monetary penalty notice

[75] DPA, s 55C(1).
[76] DPA, s 55(a).
[77] The fines are paid must be paid into the Consolidated Fund owned by HM Treasury. ICO, 'Data Protection Act 1998: Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998', 2012) 4 <http://ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_guidance_on_monetary_penalties.pdf> accessed 13 June 2014. (Hereinafter 'ICO Monetary Penalty Guidance')
[78] The ICO advises that a serious contravention of the DPA will be determined on a case by case basis, with the aim of reflecting 'the reasonable expectations of individuals and society and ensure that any harm is genuine and capable of explanation. It is possible that a single breach may be sufficient to meet this threshold.' A specific example given of a 'serious' breach of the DPA includes '[t]he failure by a data controller to take adequate security measures (use of encrypted files and devices, operational procedures, guidance etc.) resulting in the loss of a compact disc holding personal data.' ICO, 'Monetary Penalty Guidance' 13.
[79] ICO, 'Monetary Penalty Guidance' 4.
[80] ICO, 'Monetary Penalty Guidance' 14-15.

should act as an encouragement towards compliance, or at least as a deterrent against non-compliance, on the part of all data controllers or persons'.[81]

As such, the ICO's issuance of monetary penalties, which is an important part of the *regulatory* framework, arguably *does* recognise and provide for harms affecting broader, public interests. Issuing monetary penalties to promote general compliance with the DPA's principles recognises the broader public interests at stake if personal data are not treated accordingly. Furthermore, the monetary penalties operate as a sanction or penalty for sub-standard data processing. Sanctions and penalties will be assessed for effectiveness as a deterrent to harmful (or potentially harmful) data processing in Section 9 *Implications*.

This understanding of the narrow, legal framework within which harm is *legally* recognised provides the necessary backdrop from which the hard evidence can be understood. This brief overview has highlighted the value added from the soft evidence, which provides a more holistic understanding of the types of harms that *should* be recognised and provided for (as opposed to what *is* legally recognised) when processing health or biomedical data.

3.C Harm in other contexts

Here we look at harm, specifically damage and distress, in the wider, psychosocial context. The term 'distress' covers an array of negative emotional states such as feelings of hopelessness, despair, anger, shock, sadness, guilt and shame, and all of these states, as we argue later, are perceived/subjective.

To clarify at the outset, those who are affected by data breaches could be referred to as targets or victims. However, in this review we refer to those affected as subjects. Although this term strays away from psychology, we use it because it is neutral and bears no relevance on whether the abuse is intentional and deliberate or not. Harm can take several forms, such as financial, legal, physical, social and psychological. The subject of a harmful action can experience more than one form of harm resulting from that action. For example, if an individual living with HIV has been the subject of a data breach and the HIV status becomes known to others, he or she can experience social harm in that colleagues/neighbours avoid or disparage the subject, and psychological harm in that such experiences cause upset and distress. If that individual in addition then becomes unemployed (e.g. constructive or unfair dismissal), financial harm also comes into play, and this could culminate in existential fear.

It goes beyond the remit of this report to discuss individual, intra- or intergroup processes, emotions and coping strategies in any depth. This section is to be understood as a brief excursion into the disciplines of individual and social group psychology, where we draw on the

[81] 'Data Protection Act 1998: Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998' 5.

highly cited literature of acknowledged authorities. Below we discuss the subject as (a) a unique individual with a personal identity and as (b) a member of a social group with a social identity.

3.C.1 Personal identity and coping mechanisms

As individuals, we each have a unique personal identity and there is an array of inherent personality factors that may influence how well we deal with specific situations. Therefore nature sets out to some degree who we are and who we could become. At the same time our upbringing, social circumstances, interactions with peers etc. can influence our beliefs, attitudes etc. Therefore, nurture too plays a role in who we are and who we could become. It is generally acknowledged that there is an interaction between nature and nurture (although it is still very much under debate which of the two is more influential).[82]

Thus, individuals differ in how well they are equipped to cope with the stress resulting from a challenging situation,[83] and this ability can change over the lifespan.[84] Further, coping strategies can range from adaptive in that the individual pursues a course of action that is useful to him/her (e.g. seek qualified advice, take action) to maladaptive in that the individual pursues a course of action that has a detrimental effect on him/her (e.g. alcohol consumption, revert to the powerless victim role).[85] A subject might employ both mechanisms over time.[86]

3.C.2 Social identity and vulnerable social groups

In addition to unique personal identities, simultaneously we have a series of social identities. These are based on our memberships in social groups, for example age-based, gender-based and ethnicity-based. Some of these social groups can be considered vulnerable, and some individuals possess more than one vulnerable social identity (e.g. an older female living with a chronic condition in an area high in social deprivation). In this sense, an individual can experience multiple disadvantages based on social group memberships. For the purpose of this review, we refer to those who are vulnerable (multiple) group members as belonging to lower-power/lower-status groups. In doing so, we draw on Social Identity Theory, a European-based model developed since the late 1970s.[87] This model has currency and seems to offer a very

[82] See, for example, Thomas J Bouchard 'Genetic Influence on Human Psychological Traits: A Survey' (2004) 13:4 Current Directions in Psychological Science 148-151; cf Arnold Sameroff 'A Unified Theory of Development: A Dialectic Integration of Nature and Nurture' (2010) 81:1 Child Development 6-22.
[83] Richard Lazarus and Susan Folkman, *Stress, Appraisal, and Coping* (Springer Publishing 1984); Igor Kardum and Jasna Hudek-Knežević, 'The relationship between Eysenck's personality traits, coping styles and moods' (1996) 20:3 Personality and Individual Differences 341-350; Richard Lazarus, 'Toward better research on stress and coping' (2000) 55:6 American Psychologist 665-673; Julie Penley and Joe Tomaka 'Associations among the Big Five, emotional responses, and coping with acute stress' (2002) 32:7 Personality and Individual Differences 1215-1228.
[84] Susan Folkman et al, 'Age differences in stress and coping processes' (1987) 2:2 Psychology and Aging 171-184.
[85] Charles Carver et al, 'Assessing coping strategies: A theoretically based approach' (1989) 56:2 Journal of Personality and Social Psychology 267-283.
[86] Richard Lazarus and Susan Folkman, 'Coping as a mediator of emotion' (1988) 54:3 Journal of Personality and Social Psychology 466-475.
[87] Henri Tajfel, 'Social identity and intergroup behaviour' (1974) 13:2 Social Science Information 65-93; 'Interindividual behaviour and intergroup behaviour' in Henri Tajfel (ed), *Differentiation between social*

plausible explanation for (inter-)group processes in neo-liberal societies such as ours (e.g. Australia, Europe, North America).

3.C.3 Higher-power/higher-status groups

Strong evidence suggests that the quality of the relationship between a higher-power/higher-status and a lower-power/lower-status social group is determined by the interaction between perceived status, legitimacy and stability,[88] as well as power differentials between these.[89] Generally, the higher the status, the higher the power. A more powerful group may abuse its power, because it has not only the *ability* but also the *means* to do so. An example of this might be senior NHS management falsifying waiting list times. When a lower-power/lower-status group questions the legitimacy of the higher-power/higher-status group, it might be moved into taking action. An example of this is the collective action resulting in the formation of the group The Big Opt Out.[90] However, it is often the case that a lower-power/lower-status group may not be in a position to challenge realistically the higher-power/higher-status group or the status quo. An example here would be a Health Board ignoring complaints to the degree where the complainant simply 'gives up trying'.

3.C.4 Lower-power/lower-status groups

Given that each social group is, broadly speaking, anchored in its own norm-specific culture, here we give three examples (older people, IV-drug users, Black and Minority Ethnic citizens) of specific psychosocial challenges and beliefs that may co-determine how well the lower-power/lower-status group member is equipped to deal with an abuse.

Research suggests that some older people might feel that they do not deserve to be treated as well as younger people.[91] Firstly, ageist attitudes may have been internalised and therefore the belief that younger individuals are more entitled to better treatment that they are. Secondly, older people are or might be more likely to accept the status quo that institutional power is

---

groups: Studies in the social psychology of intergroup relations (Academic Press 1978) 27-60; Henri Tajfel and John Turner 'An integrative theory of intergroup conflict' in William Austin and Stephen Worchel (eds), *The social psychology of intergroup relations* (Brooks/Cole 1979) 33-48;
Henri Tajfel and John Turner 'The social identity theory of intergroup behaviour' in Stephen Worchel and William Austin (eds), *Psychology of intergroup relations* (Nelson-Hall 1986). For the most current developments and thinking regarding Social Identity Theory, see: Matthew J Hornsey and Michael A Hogg 'Assimilation and diversity: An integrative model of subgroup relations' (2000) 4:2 Personality and Social Psychology Review 143-156; 'The effects of status on subgroup relations' (2002) 41 British Journal of Social Psychology 203-218.

[88] John C Turner and Rupert J Brown 'Social status, cognitive alternatives and intergroup relations' in Henri Tajfel (ed), *Differentiation between social groups*.

[89] Although power and status are similar, these are two distinct constructs. Power is defined typically, as 'the degree of control one group has over its own fate and that of outgroups' (Jones, 1972, 416). Status reflects the standing a group has within an intergroup setting. It can be expressed in terms of prestige, power, privileges and so forth (Hornsey et al, 2003). James M Jones *Prejudice and racism* (Addison-Wesley 1972); Matthew J Hornsey et al, 'Relations between high and low power groups: The importance of legitimacy' (2003) 29:2 Psychology and Social Psychology Bulletin 216-227.

[90] 'TheBigOptOut.Org' <http://www.thebigoptout.com/about-nhs-confidentiality/> accessed 18 June 2014.

[91] British Institute of Human Rights, *Your human rights: A guide for older people* (2nd ed, British Institute of Human Rights 2010).

unquestionable. Thirdly, they are part of the 'make do and mend' generation, so whether subjects would seek restorative justice is questionable.

Intravenous drug users are, by definition, criminalised in our society. Some are high functioning (i.e. maintain employment and residence), and the emotion of shame and/or fear of prosecution might hinder them in seeking restorative justice.

Black and Minority Ethnic groups can be multiple disadvantaged, and seeking restorative justice might be less likely. Namely, some might be embedded in a collectivist and not an individualist culture, be confronted with linguistic barriers and lack knowledge of rights and complaints procedures.

3.C.5 Perpetrators and prejudice/discrimination

The Equality Act 2010 seeks to protect individuals with protected characteristics from discrimination in the workplace and in wider society. According to the Act, discrimination can be direct or indirect, taking the form of harassment or victimisation. However, discrimination (the act or behaviour) is fuelled by prejudicial beliefs and attitudes (the 'rationale' for such acts or behaviour), and these in the main can take two forms. Blatant prejudice is 'hot, close and direct', whilst subtle prejudice is 'cool, distant and indirect'.[92] In the context of this report, prejudice is more likely to be subtle. Tactics involve rejecting the subject (and his/her social group) for reasons that are apparently non-prejudicial (for example, a public consultation that pays lip service only). Some perpetrators act alone, others in groups – indeed, some with organisational backing such as is the case with institutional discrimination. It is notoriously difficult to prove instances of indirect, subtle discrimination, particularly because it may comply with social norms.[93] Further, the discrimination might not be hostile, but benevolent, that is, 'we are doing this for your own good'.[94]

3.C.6 The harm versus the impact

We do not dispute that there might be cases where subjects of data breach feel 'no harm done' (in legal terms, no actual harm). A hypothetical example: were a dentist to lose a patient's record, one individual might be satisfied if a new set of x-rays were taken. Another – with HIV-positive status – might be very distressed at the loss. From this, we propose that the actual harm (the lost dental record) can have two entirely different impacts. The impact itself can range from mild/benign to severe/traumatic. In broadest terms, there are two explanations for this. Firstly, the effect experienced is based on the subject's individual and social identities, as well as their personal circumstances, life stories, etc. In this sense, it is wholly correct to refer to

[92] Thomas Pettigrew and Roel Meertens, 'Subtle and blatant prejudice in western Europe' (1995) 25:1 European Journal of Social Psychology 57-75.
[93] Thomas Pettigrew and Roel Meertens, 'Subtle and blatant prejudice in Western Europe'; 'Is Subtle prejudice really prejudice?' (1997) 61: Public Opinion Quarterly 54-71.
[94] Peter Glick and Susan Fiske, 'The Ambivalent Sexism Inventory: Differentiating hostile and benevolent sexism' (1996) 70 Journal of Personality and Social Psychology 491-512.

'perceived distress', because it is subjective. Secondly, the degree of perceived distress is linked to an individual's coping strategies, which again are linked to their individual identity, lived experiences etc.

3.C.7 Impact in the psychosocial context

It is clear, then, that several factors need to be considered if we are to shed light on what harm and distress can mean in social reality terms, and if and how subjects can be protected, supported and, perhaps, compensated. Data protection law (or other laws) offer redress for incidents that (some) subjects have experienced and, potentially, which have changed their circumstances? Financial harm (damages) is recognised by the courts, but it seems that the legal notion of 'distress' goes no way to describing the pain and misery that subjects of discrimination, stigmatisation or other harms can suffer.[95]

We conclude here:

1. The subject has financial recourse for distressed suffered only if the breach has resulted in financial harm or can casually connect the distress suffered to the use of their data in journalism, literature or the arts (for the 'special purposes' under the DPA). Both options go no way to covering psychosocial harm that a subject might experience.
2. It is acknowledged that two factors interact in determining how well an individual might be able to cope with an adverse situation.[96] One of these is 'perceived control'. If there is no *feasible* or *realistic* course of action available to a subject, perceived control will be low and this can diminish the ability to cope significantly.
3. Some subjects will not come forward, because they do not personally perceive any harm, do not feel it is their right to come forward, have too many stressors to deal with that this would increase their stress and/or feel too disempowered to come forward. Here it is in the hands of the law to protect such individuals.
4. Because distress is a subjective experience, it could be argued that it is in the hands of the subject and not the law to decide what constitutes harm or not.
5. However, there are limits in how the law both recognises and compensates for harms caused. Arguably, this neglects the broader spectrum of harms that the psychosocial dimension elucidates.

[95] However, the individual data subject can recover for suffering distress if either of the requirements under s 13 of the DPA are met – namely – if (a) the individual also suffered damage (financial) as a result of the contravention of the Act; or (b) if the individual suffered their distress due to the use of their data in journalism, literature or art (the "special purposes"). DPA, s 13(a),(b).

[96] Sheldon Cohen and Thomas A Wills 'Stress, social support, and the buffering hypothesis' (1985) 98:2 Psychological Bulletin 310-357.

Actual harm – versus impact:

The remit of this report was to identify ‘actual harm’. It is contended that this is not possible in the psychosocial context because subjectivity is key. For this reason we refer to the ‘harms’ identified in the soft evidence (newspaper) review, as “impact” which can range from none at all, to mild irritation, to extreme distress. Therefore the term ‘impact’ is used in Sections 7.B.2 Soft evidence typology and 8.B Soft evidence.

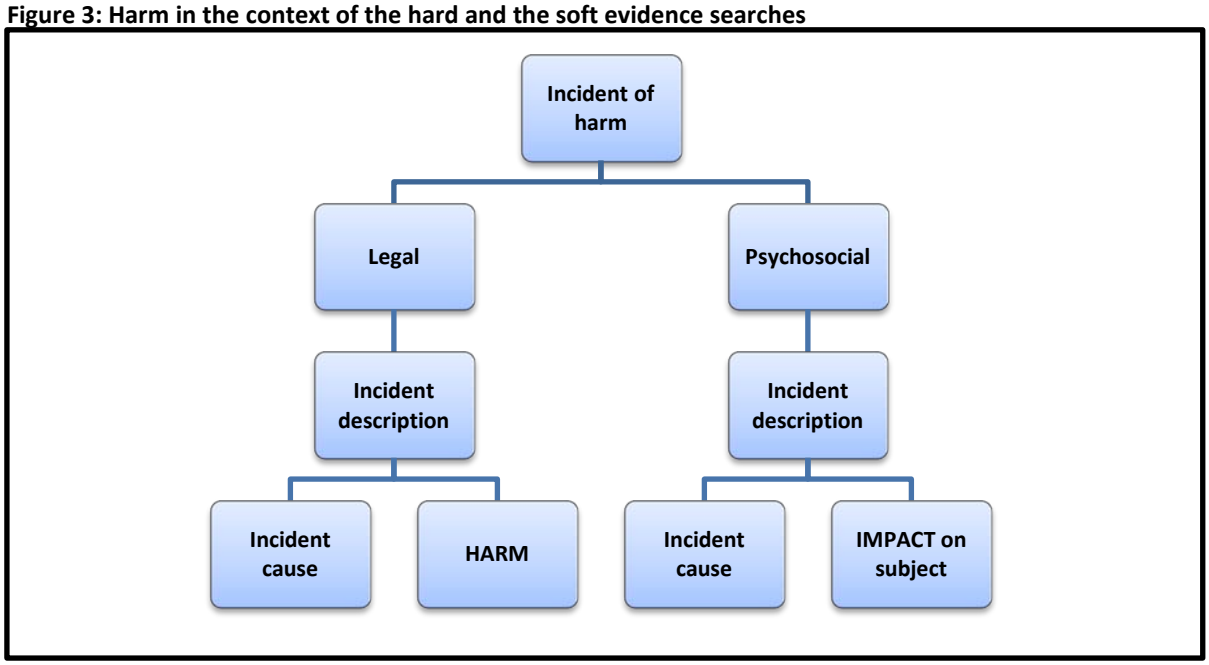
4. Abuse and harm – categories, causes and impact

In Section 3.B we considered harm as it is understood in the narrower, regulatory context and the related procedures for seeking legal compensation for damage or distress. In Section 3.C the concept of harm was considered through the wider lens of social reality. At this point it is essential to present our understanding of categories of abuse, its causes and the impact it can have or harm it can cause.

For the purposes of this evidence review, it was crucial to adopt a conception of harm that encapsulated ***both*** the legal *and* the psychosocial dimensions. Thus as indicated in Figure 3 below, from this common starting point we could identify an incident, examine its cause and any harm to an individual or public interest, within and outside of the constraints of the legal. We counted an incident as hard or soft evidence if it:

- involved health or biomedical data[97],
- irrespective of whether the data was digitalised or in paper-based form, and
- represented harm[98] arising from data use or non-use[99].

Figure 3: Harm in the context of the hard and the soft evidence searches



[97] As defined in 3.A.1 above.
[98] Harm as understood in the narrower, legal context as well as the broader, psychosocial context as described in Section 3.C as 'impact'.
[99] Non-use refers to any opportunity costs to institutions or individuals of not sharing or linking data.

Evidence of harm was then considered in terms of the *'abuse'* of health or biomedical data. Terminology such as 'breach' implied *use* of data and the brief was to conduct an evidence review for harms arising both from use *and* non-use of data. Non-use refers to missed opportunities from the failure to use data resulting in e.g. suboptimal use of data from the point of view of the development of scientific knowledge, securing health outcomes, promoting economic growth and wider public benefits, etc. Thus 'abuse' was used to refer to both data breaches and cases of non-use in the typologies developed.

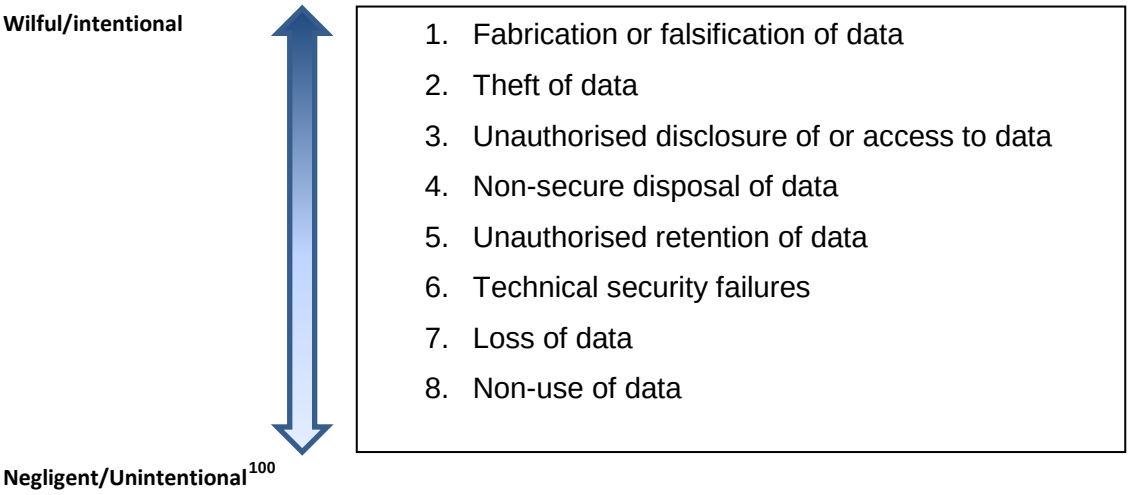
Against this backdrop, it became apparent that data could be abused in the legal sense, whilst in the psychosocial sense the abuse of data does not necessarily result in harm to the individual – and where it did, the consequences could be devastating. We felt that merely the consistent use of the term 'breach' would imply use of data, rather than any resultant harm to the subject. Therefore, we searched broadly for incidents involving health or biomedical data, using terms of reference such as data breach but also for specific instances of *non*-use. In other words, to bring the legal and psychosocial perspectives together for the purposes of this evidence review we searched for incidents of 'harm' as they arose from:

1. **Abuse of data, and/or**
2. **Non-use of data.**

4.A Categories of abuse

We were mindful of the types of abuse mentioned in the Brief for Tender, but we did not seek to allocate incidents into pre-determined categories of abuse. Rather, we let the data speak for themselves (the inductive approach). As shown in Figure 4 the types of abuse uncovered in this evidence review broadly include:

Figure 4: Types of abuse



[100] Failure to use data (*non*-use of data) is admittedly considered separately from the types of abuse that arise from actual *use* of data given a) the overall lack of evidence found on harms arising from failure to use health or biomedical data and b) the broader nature of harms that could stem from *non*-use e.g. stunting the development of scientific knowledge etc., as opposed to the individual harms uncovered and arising from *use* of data.

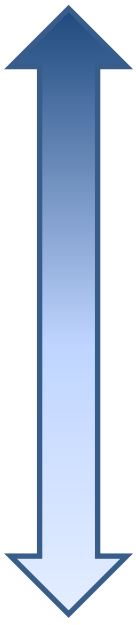
After a team discussion the categories of abuses identified were ranked on an ordinal scale ranging from wilful and intentional abuses of data to more unintentional or negligent uses – both of which can result in harm/impact for individuals, organisations or broader public interests. Importantly, this spectrum of abuse is ***not*** exhaustive – it is informed by the data.[101]

4.B Causes for abuse

The abuse of health or biomedical data was then attributed to a 'cause' that may be understood as an incentive or motivation leading to harm or impact. Linking the abuse to a specific cause was likewise subject to team discussion. There were differences in how easily a cause could be established, whereby and as expected, the hard evidence gave a clear understanding of the cause, whereas the soft evidence did not. There were other differences in the categorisation processes. For instance, the soft evidence findings showed that it would be useful to distinguish cause by involvement with NHS staff versus those incidents not involving NHS staff; whereas the hard evidence did not require such a distinction due to the wider variety of incidents found. As shown in Figure 5 these causes broadly include:

Figure 5: Causes for abuse of data

Wilful/intentional



Negligent/unintentional

- Abuse of data to meet NHS/organisational objectives
- Abuse of data to protect professional reputation
- Abuse of data for self-gain (e.g. monetary gain)
- Abuse attributed to third parties (e.g. hackers)
- Disclosure by the press or media
- Unauthorised access without clinical or lawful justification (e.g. for curiosity)
- Against the wishes/objections of the individual
- Abuse as a result of insufficient safeguards
- Abuse arising out of a Freedom of Information request
- Abuse due to maladministration (e.g. failure to follow correct procedures)
- Abuse due to human error (e.g. sending a fax to the wrong recipient)
- Non-use due to misinterpretation of legal obligations

The causes attributed to abuse or non-use of data are also ranked on an ordinal scale by the team, from wilful and intentional abuses of data by the data controller/their staff, moving towards

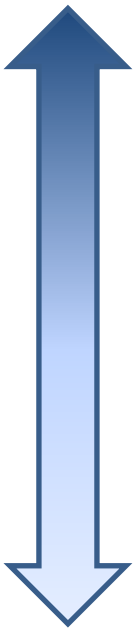
[101] In Section 10.E we consider the possibility for future work to take forward an evidence review specific to threats, vulnerabilities, risks and potential mitigations whereas this commission focused on evidence of *actual* harm and thus *incidents* (as opposed to risks contributing to abuses of data).

involvement of third parties,[102] and less intentional, more negligent use or non-use of data that can nevertheless be harmful to individuals or broader, public interests.

4.C Harm types

Finally, we considered 'harm' in terms of individual harm, harm to institutions (including harm to an organisation's reputation or diminishing public trust in the confidentiality of the doctor-patient relationship etc.), potential for harm in the future, and findings of *no* harm (from the perspective of the evidence source i.e. the perspective of a judge etc.). Importantly, the list in Figure 6 below is *not* exhaustive as to the types or range of harms that could potentially befall an individual or organisation as a result of the abuse of health or biomedical data. Rather, the types of harm in Figure 6 are specifically and informed by the data we gathered in this review:

Figure 6: Harms caused by abuse



- Receipt of suboptimal care, resulting in detriment to health or death
- Individual distress e.g. emotional, physical, etc.
- Damage to individual reputation (e.g. societal, personal or professional)
- Individual, financial loss
- Damage to public interest (e.g. loss of faith in confidential, health service, general loss of public trust in medical profession, delayed or stunted scientific progress etc.)
- Damage to organisational reputation (e.g. to NHS)
- Potential for harm to individual, organisation or the public interest in future
- No evidence of harm found due to lack of reported information

Importantly, this spectrum of harm includes incidents where there was simply not enough information reported on the nature of the abuse to describe harm caused to either an individual, organisation or broader public interest. Such incidents were found typically in the soft evidence **(**newspaper and social media) review. In Section 9.A we will consider the implications from findings of 'no evidence of harm' as well as the *lack* of evidence for types of harm not uncovered (or thus reflected in Figure 6 above).

[102] Abuse attributed to the actions of a third party, such as a hacker, can implicate both the wilful/intentional abuse by the third party as well as, potentially, the negligence of the data controller who may have been able to prevent the abuse through more stringent, technical security/safeguards etc.

‘No evidence of harm’:

For the purposes of this review, where an incident is categorised with ‘no evidence of harm’, this does ***not*** indicate that the individual, organisation and/or public interest did not in fact suffer harm. Rather, ‘no evidence of harm’ merely reflects that the incident was not reported with sufficient detail for us to meaningfully describe the nature of 1) the incident and 2) the type of harm that may have been caused.

5. Approach/Methodology

Please note: Contrary to convention but at the request of the Nuffield Council on Bioethics (NCOB) Working Party on Biological and Health Data and the Expert Advisory Group on Data Access (EAGDA), this section appears at the start of this document and not before the Method section.

This includes the sub-sections:

- Scope
- Methodology
- Limitations.

6. Method

Note: All searches described below took place between February and March 2014.

6.A Hard evidence

The hard evidence strand encompassed a systematic review of court and tribunal rulings from the UK, the European Court of Human Rights (ECtHR), and the Court of Justice of the European Union (CJEU), as well as the administrative enforcement measures undertaken by the ICO. This compilation of resources provided a firm evidence base on the sanctions aimed at addressing abuses of health or biomedical data, from the standpoint of laws protecting the range of data and privacy interests at stake, including the DPA and common law provisions such as breach of confidence.[103] The databases used for the hard evidence search were primarily UK focused, although ECtHR and CJEU cases were searched to seek parallel cases of abuse in the EU. As a systematic search method was employed, evidence was limited to incidents found under the search criteria and other search parameters chosen (i.e. timeframe, database chosen).

The websites searched are shown in
Table 4 below. For more in-depth details on the constraints encountered in each website, see Appendix, Table 22.

[103] This refers to the overlap between breaches of the DPA, and actions at common law, namely, breaches of confidence (also understood post-enactment of the Human Rights Act as misuse of private information). There was further regulatory overlap in court judgments, where the European Convention of Human Rights, and in particular Article 8, was often implicated if the abuse of data involved a breach of an individual's right to private and family life.

Table 4: Hard evidence: websites consulted

Site	Time frame	Search terms
UK Case Law within LexisNexis: http://www.lexisnexis.com/uk/legal/	1998-2014	'health or medical PRE/1 data and breach' 'biomedical and data' 'biological data' 'genetic and data and breach' 'health and data and non-use'
UK Information Tribunal Cases: http://www.informationtribunal.gov.uk/Public/search.aspx	-	**jurisdictional area 'DPA 1998'** 'sensitive personal data' 'confidentiality of information' 'right to prevent processing likely to cause damage or distress' **jurisdictional area 'HRA 1998'** 'right to private and family life' **jurisdictional area 'FOI 2000'** 'information provided in confidence'
UK Information Commissioner's Office Prosecutions, Monetary Penalty Notices and Decision Notices: http://ico.org.uk/enforcement	-	**Prosecutions and Monetary Penalty Notices:** no search terms used; read case by case **Decision Notices:** 'health data', 'biomedical data'
EU Case Law within LexisNexis: http://www.lexisnexis.com/uk/legal/	1995-2014	'health or medical PRE/1 data and breach' 'genetic or biomedical and data and breach' 'biological data' 'health and data and non-use'

6.B Soft evidence

In terms of the soft evidence strand, the search to establish evidence of abuse and its impact from the standpoint of the subject or the subject's group required flexibility and creativity. The search engine used was Google, where identified sites were explored and relevant sites emerging from the original sites were explored further. The sites (see Table 5 below) identified as a starting point were (a) newspapers in the UK, (b) charitable organisations representing the most vulnerable and therefore potential subject groups of discrimination and (c) 'citizens' voice' sites, which were identified through the newspaper searches.

Table 5: Soft evidence – list of newspaper, charity and citizens' voice websites

Newspapers	Charities	'Citizens' Voice'
Express	Age UK	Big Brother Watch
Guardian	Carers UK	Citizen's Advice
Independent	Lesbian and Gay Foundation	Digital Right Ireland
Mail	Mind	GeneWatch
Mirror	Prisoners' Advice Service	Healthwatch
Sun	Prison Reform Trust	Liberty
Telegraph	Race Equality First	medConfidential
Times	Race Equality Foundation	Patients' Association
Belfast Telegraph (NI)	Stonewall	Patient Care (Watchdog)
The Herald (Scotland)	Terrence Higgins Trust	Patient Concern
Western Mail (Wales)		

Search terms*	Search terms*	Search terms*
medical; *patient*; *record*; *data*; *breach*; *misuse*; *biomedic*; *genetic*	*data, breach* and/or *misuse*	*data, breach* and/or *misuse*

*Note that there were many differences in search options between these sources, such as the use of Boolean operators, searching specific sections, searching specific time spans.

As listed in Table 6 below, the UK on-line newspapers (including Northern Ireland, Scotland and Wales) were chosen because of their high circulation figures and the range of demographic readerships, inclusive of daily and Sunday editions. The search covered the longest time span that was available. The charities chosen represent the most exposed groups in society who are vulnerable to discrimination and/or stigmatisation. The citizens' voice groups were identified, because they were cited in certain newspaper articles.

Table 6: Newspapers, charities and citizen's voice groups

Newspapers	Web-site	Type	Circulation[104]	Readership
Express	http://www.express.co.uk/	middle-market	529,648	right-wing, populist
Guardian	http://www.theguardian.com/uk	(former) broadsheet	204,440	centre-left, social liberal
Independent	http://www.independent.co.uk/	compact	76,802	economically liberal, politically centrist
Mail	http://www.dailymail.co.uk/news/index.html	middle-market	1,863,151	right-wing, populist
Mirror	http://www.mirror.co.uk/	tabloid	1,058,488	social-democratic, populist
Sun	http://www.thesun.co.uk/sol/homepage/	tabloid	2,409,811	right-wing, populist
Telegraph	http://www.telegraph.co.uk/	broadsheet	555,817	centre right, conservative
Times	http://www.thetimes.co.uk/tto/news/	broadsheet	399,339	centre-right
Belfast Telegraph (NI)	http://www.belfasttelegraph.co.uk/	compact	53,847[105]	In NI context, 'balanced'[106]
The Herald (Scotland)	http://www.heraldscotland.com/	broadsheet	47,226[107]	centre-left
Western Mail (Wales)	http://www.walesonline.co.uk/	compact	32,926[108]	populist
Charities	**Web-site**	**Purpose**		
Age UK	http://www.ageuk.org.uk/	The largest UK organisation dedicated to 'inspire, enable and support' older people. Remit: from financial advice to health and wellbeing support.		
Carers UK	http://www.carersuk.org/	To support those looking after family/friend who is older, disabled or seriously ill. Remit: from debt advice to dealing with caregiver burden		
Lesbian and Gay Foundation	https://www.lgf.org.uk/	To advise and support lesbian, gay and bisexual people. Remit: from coming out advice to dealing with sexual violence		
Mind	http://www.mind.org.uk/	To advise, support and empower anyone experiencing a mental health problem. Remit: from information on drugs and medication to legal rights.		
Prisoners' Advice Service	http://www.prisonersadvice.org.uk/	To provide legal advice and information to prisoners in England and Wales. Remit: from temporary release to mother and baby units.		

[104] 'List of newspapers in the United Kingdom by circulation' <http://en.wikipedia.org/wiki/List_of_newspapers_in_the_United_Kingdom_by_circulation> adapted from the Audit Bureau of Circulation (access with subscription only), accessed 17 April 2014.
[105] ABC, 'Belfast Telegraph ABC Audited Figures' <http://www.abc.org.uk/Products-Services/Product-Page/?tid=20868> accessed 29 April 2014.
[106] TGI, <http://www.tgisurveys.com> accessed 29 April 2014.
[107] Jamie McIvor, 'Scottish daily paper sales slip' (2011) <http://www.bbc.co.uk/news/uk-scotland-14509435> accessed 29 April 2014.
[108] ABC, 'Audit Bureau of Circulation: Summary Report - The Western Mail' (2009) <http://www.abc.org.uk/Products-Services/Product-Page/?tid=20940&epslanguage=en-GB> accessed 29 April 2014.

Prison Reform Trust	http://www.prisonreformtrust.org.uk/	To inform prisoners, to influence the Judiciary and the Executive. Remit: from citizenship to prisoners with learning difficulties.
Race Equality Foundation	http://www.raceequalityfoundation.org.uk/	To explore discrimination and disadvantage, in order to develop interventions. Remit: from health to gun and knife gang crime.
Stonewall	https://www.stonewall.org.uk/	A major campaigner and lobbyist, representing the lesbian, gay and bisexual community. Remit: from education to health.
Terrence Higgins Trust	http://www.tht.org.uk/	To promote sexual health, minimise HIV rates, to empower those living with HIV. Remit: from sexual health education to immigration and healthcare.
Citizens' Voice groups	**Web-site**	**Purpose**
Big Brother Watch	http://www.bigbrotherwatch.org.uk/	To challenge policies that threaten privacy, freedom and civil liberties
Citizen's Advice	http://www.citizensadvice.org.uk/	To provide advice on issues such as debt, employment, housing and discrimination
Digital Right Ireland	http://www.digitalrights.ie/	To defend civil, human and legal rights in a digital age.
GeneWatch	http://www.genewatch.org/	To monitor developments in genetic technology development (not only) from the public interest perspective
Healthwatch	http://www.healthwatch.co.uk/	To deliver the consumer voice to the commissioners, regulators and providers of health and care services. England only. Has statutory powers.
Liberty	http://www.liberty-human-rights.org.uk/	To campaign to protect basic rights and freedoms through the courts, in Parliament and in the wider community.
medConfidential	http://medconfidential.org/	To campaign for confidentiality and consent in health and social care
Patients' Association	http://www.patients-association.com/	To advocate for better access to accurate and independent information for patients and the public, and for patient rights and decision-making
Patient Concern	http://www.patientconcern.org.uk/	To promote choice and empowerment for all health service users

6.C Twitter evidence

The method for searching for evidence on social media began with a search for the world's most popular social media website, Facebook (as ranked in March, 2014).[109] However, due to the way Facebook's privacy settings are enabled, the search conducted would not return any relevant hits within the profiles of individuals, that is, hits that were native to the Facebook website. Rather, Facebook conducted the search automatically via Google's search engine. [110]

Therefore, the second most popular social media site – Twitter – was used. Twitter's advanced search function was employed for the terms 'health data breach', excluding the words 'care.data'. This search returned over 1,000 hits, whilst the search for 'biomedical data breach', 'biological data', and 'genetic data breach' excluding care.data returned no hits.[111] The search was revised to search for: 'medical data breach', excluding the words 'care.data' and limiting the search to tweets posted within Scotland, UK as medical was determined to be a more common and less technical term suited to the social media nature of Twitter.[112]

[109] As of 7 March 2014, Facebook received an estimated 900,000,000 unique monthly visitors, whereas Twitter received 310,000,000 and LinkedIn 250,000,000. eBizMBA, 'Top 15 Most Popular Social Networking Sites March 2014' (2014) <http://www.ebizmba.com/articles/social-networking-websites> accessed 27 March 2014.

[110] As a result a search was conducted via Facebook's general search bar, whilst being logged in under an individual user profile. The terms 'health data breach', 'medical data breach' and 'biomedical data breach' were searched for and returned no hits which were 'native' to the Facebook website.

[111] Due to space constraints and to facilitate data analysis the search was narrowed.

[112] Scotland, UK as opposed to the entirety of the UK was chosen as the limiting variable to the search because it was not possible to select tweets posted from within the whole UK – only specific cities, zip codes or countries.

7. Results

Under 6.A, initial findings are presented from the hard evidence, the soft evidence and Twitter, where we discuss frequencies and percentages. Under 7.B, we present the emergent typologies of abuse, cause and harm, where findings are differentiated by abuse type, and cross-matched by cause and by harm/impact. Under Section 7.C the merged evidence is presented.

7.A Initial findings

7.A.1 Hard Evidence

The hard evidence uncovered 705 total hits, of which fifty-one incidents fit the criteria as hard evidence of abuse of health or biomedical data (see Table 7 below). Each incident was assigned a unique incident number (e.g. UKC1, ICOP1 etc.), case name (where appropriate), date, source, abuse type (with synopsis of the incident), cause and synopsis on the harm caused (if any evidence of harm was indicated). A detailed list of the fifty-one relevant hits is provided in Table 23 of the Appendix.

Table 7: Hard evidence results

Target	Time frame	Search terms	Total hits	Relevant hits
UK Case Law[113] **within LexisNexis**	1998-2014	'health or medical PRE/1 data and breach'	65	14 (20%)
		'health and data and non-use'[114]	33	0 (%)
		'biomedical and data'	34	0(0%)
		'biological data'	4	0 (0%)
		'genetic and data and breach'	147	0 (0%)
		Total hits for UK Case Law:	**283**	**14 (5%)**
UK First-tier Tribunal	-	**jurisdictional area 'DPA 1998'**		
		'sensitive personal data'	6	0 (0%)

[113] All cases searched from Privy Council, Supreme Court, House of Lords, Court of Appeal (All), CA, Civil Division, CA, Criminal Division Family Division, Queen's Bench Division (All), QBD, Administrative Court, QBD, Admiralty Court, QBD, Commercial Court, QBD, Divisional Court QBD, Technology and Construction Court, Chancery Division (All), ChD, Patents Court, ChD, Companies Court, Employment Appeal Tribunal, Lands Tribunal, Special Commissioners, VAT and Duties Tribunal, High Court of Justiciary, Scotland, Court of Session, Scotland, Northern Ireland Court of Appeal, Northern Ireland Queen's Bench Division, First-tier Tribunal (Tax), Upper Tribunal (Tax and Chancery Chamber), Competition Appeal Tribunal, Court of Protection, Upper Tribunal (Administrative Appeals Chamber), Upper Tribunal (Immigration and Asylum Chamber), Upper Tribunal (Lands Tribunal).

[114] The search for *non*-use of data was expanded to incorporate *all* case law available in the LexisNexis database. Thus these results (0 relevant hits) for non-use reflect both UK and EU case law.

Target	Time frame	Search terms	Total hits	Relevant hits
(Information Rights)[115] cases:		'confidentiality of information' 'right to prevent processing likely to cause damage or distress'	2 3	0 (0%) 0 (0%)
		jurisdictional area 'HRA 1998' 'right to private and family life'	 4	 1 (25%)
		jurisdictional area 'FOI 2000' 'information provided in confidence' **Total hits for Information Tribunal:**	 8 23	 0 (0%) 1 (4%)
UK Information Commissioner's Office Prosecutions, Monetary Penalty Notices and Decision Notices	-	**Prosecutions:** read case-by-case **Monetary Penalty Notices:** read case-by-case **Decision Notices:** 'health data' and 'biomedical data' **Total hits for ICO enforcement:**	17 51 6 **74**	4 (24%) 14 (27%) 6(4) (6%) **22 (30%)**
EU Case Law[116] within LexisNexis Database	1995-2014	'health or medical PRE/1 data and breach' 'genetic or biomedical and data and breach' 'biological data' **Total hits for European case law**:	271 47 7 **325**	13 1 0 (0%) **14(4%)**
Cumulative Total			**705**	**51 (7%)**

Of the 283 total UK case law hits a mere 5% were relevant, fitting the criteria for hard evidence. Out of the total fourteen relevant incidents found in UK case law *all* fourteen related to health data.

The First-tier Tribunal cases considered only uncovered twenty-three relevant hits, of which only one (4%) was relevant.

The ICO enforcement measures uncovered more relevant hits by percentage compared to any other source considered because of the narrow focus of the ICO on *data*-related incidents. Out of a total seventy-four hits, 30% of these met the hard evidence criteria, with monetary penalty notices carrying the most hits and most *relevant* hits (4%: fourteen), with prosecutions and decision notices both providing four relevant hits.

Finally, the European court judgments reviewed had the most top-level hits, producing 325 cases to consider. However, only 4% were relevant and met the hard evidence search criteria (fourteen incidents), all of which were from the ECtHR. This was expected given the role played by Article 8 protections of privacy, by virtue of the European Convention on Human Rights. Only one hit involved genetic data.(EUC7) We consider this case separately and in depth in Section 9.A.7 Genetic data as well as highlighting abuse of genetic data as an area warranting further and future research in Section 10.D.

[115] In 2010 the 'Information Tribunal' became part of the General Regulatory Chamber of the First-tier Tribunal, and thus is now named the First–tier Tribunal (Information Rights), as part of the restructuring of the Tribunal system, mandated by the Tribunals, Courts and Enforcement Act 2007.
[116] The European searched included judgments from: the Court of Justice of the EU (CJEU), European Court of Human Rights (ECtHR), General Court of the EU (formerly CFI) and European Union Civil Service Tribunal (First Chamber).

Overall, incidents relating to health data produced significantly more results than similar searches for biomedical data. This is unsurprising, given the variability in how courts use scientific terminology – terms are often interchanged. Furthermore, whereas *health* or *medical* data are mentioned specifically in both UK and European data protection legislation, neither biomedical nor genetic data are.[117] Thus, there is even less precedent for use of these terms in the legal context.[118]

7.A.2 Soft evidence

7.A.2.A Newspapers

In we list the search conditions and number of hits for each newspaper. The number of hits were categorised initially and broadly as 'abuse' or 'other'. The types of a*buse* were those indicated in Figure 4 (i.e. data loss, data theft etc.), and were not limited to specific types of data (i.e. electronic and/or hard-copy). The category *other* comprised articles that we felt might be useful for this review.[119] Irrespective of category type, we also noted any references to (a) the ICO, (b) a FoI request, and/or (c) to other organisations that had the potential to offer more evidence of abuse and harms (citizens' voice groups, e.g. Big Brother Watch, medConfidential).

A total of 208 articles were identified initially, and given a unique newspaper identifier[120] and article number (e.g. In*x* = The Independent, Te*x* = The Telegraph). The gross total of hits revealed 139 *abuse* articles and sixty-nine *other* articles. Upon closer scrutiny, the 139 *abuse* articles were reduced to eighty-seven. Of those disregarded, thirty-four lacked relevance or detail and eighteen were re-categorised as *other*.

[117] Although there is indication from recent drafts of the pDPR that both biomedical and genetic data would be included in future data protection regulation in Europe.
[118] See Section 3.A.1 above for the definitions of health and biomedical data adopted for this evidence review.
[119] Examples include academic studies, commercial genetic testing and the phenomenon of blagging.
[120] B = Belfast Telegraph, E = Express, G = Guardian, H = Scottish Herald, In = Independent, Ma = Mail, Mi = Mirror, S = Sun, Te = Telegraph, Ti = Times, W = Western Mail.

Table 8: Search conditions and hits by newspaper

Newspapers	Advanced search	Sections searched	Hits from-to	Range of number of hits	Total initial hits	Of which 'abuse'	Of which 'other'
Express	No	News & Health	2004-2013	1-203	24	14	10
Guardian[121]	No	No	2001-2014	298-7130	27	20	7
Independent	Yes	News	2006-2014	21-551	21	14	7
Mail	No	News & Health	2008-2014	71-2451	22	10	12
Mirror[122]	No	News	2007-2014	5-429	19	14	5
Sun	No	News	2007-2013	3-2302	27	25	2
Telegraph[123]	No	News	2010-2014	≈87-≈12,100	20	5	15
Times	No	News & Health	2002-2014	9-3,182	23	17	6
Belfast Telegraph (NI)	No	News	2005-2014	0-431	18	15	3
The Herald (Scotland)	No	No	2001-2012	7-43	2	1	1
Western Mail (Wales)	No	News	2011-2013	0-627	5	4	1
Total					208	139	69

[121] Reviewed only the first 100 possible.
[122] A relevant hit was generated if the search term appeared anywhere on the webpage containing the article.
[123] Reviewed hits until message 'no more recommended' came up on the webpage.

A shown in Table 9, over half of the articles identified dated back to 2011 and 2012 (28% and 25% respectively). In terms of newspaper type, tabloid articles were the least represented (Mirror and Sun combined = 17%), middle-market (Express and Mail) and regional national (Belfast Telegraph, Herald, Western Mail) articles marginally more (18% each). Thus, half of the articles (49%) came from (former) broadsheet newspapers (Guardian, Independent, Telegraph, Times).

Table 9: Post-scrutiny abuse hits from January 2009 to March 2014 by newspaper by year

Newspapers	2014	2013	2012	2011	2010	2009	Total (%)
Express	0	2	3	1	0	3	**9 (10%)**
Guardian	3	2	2	9	0	2	**18 (21%)**
Independent	0	0	6	3	0	1	**10 (11%)**
Mail	0	0	2	2	2	1	**7 (8%)**
Mirror	2	0	0	1	0	3	**6(7%)**
Sun	0	1	3	4	1	4	**13 (15%)**
Telegraph	1	3	0	1	0	0	**5 (6%)**
Times	1	2	1	2	2	2	**10 (11%)**
Belfast Telegraph (NI)	0	4	5	2	0	2	**13 (15%)**
The Herald (Scotland)	0	0	1	0	0	0	**1 (1%)**
Western Mail (Wales)	0	2	2	0	0	0	**4 (5%)**
Total (%)	**7 (8%)**	**14 (16%)**	**22 (25%)**	**24 (28%)**	**5 (6%)**	**15 (17%)**	**87**

The net score of eighty-seven hits was inflated, because some incidents were reported in multiple newspapers and/or over several days. To rectify this, the eighty-seven articles were then sorted into a total of sixty distinct 'incidents'. We also noted which incidents were reports of multiple instances of abuse, and whether the ICO was aware of the incident or not. Please see Table 25 in the Appendix for a list of the incidents. Each incident notes the unique article number(s) such as news01, news02 and so forth, date(s) of publication, source(s) of the story (e.g. ICO, FoI, member of the public), whether the article(s) refer to multiple events, the place of the abuse (where possible), a brief synopsis of the incident and, where available, impact statements from the subjects and/or commentary statements from other organisations. We also include a separate reference list for all newspaper articles, sorted by unique article number in the Appendix Table 27.

7.A.2.B Charities and citizens' voice groups

In Table 10 we list the number of hits and relevant hits for charities and citizens' voice groups. Results from charity websites were disappointing. The search terms – *data misuse* or *breach* – did bring up 419 hits, but only one of these was relevant. This was accounted for in part by the site being closed to 'outsiders' (e.g. the Terrence Higgins Trust offers very limited access to those not living with HIV), or the site's focus (e.g. the Prison Reform

Trust, where breaches to the European Convention on Human Rights were discussed in terms of the prison population banned from voting). The only hit identified was on Age UK, informing its readership of NHS waiting-times being recorded incorrectly.

Table 10: Hits by charity and citizens' voice groups

Charities	**Number of hits**	**No. of relevant hits**	**Total**
Age UK	5	1	1
Carers UK	0	0	0
Lesbian and Gay Foundation	225	0	0
Mind	34	0	0
Prisoners' Advice Service	No search possible		
Prison Reform Trust	72	0	0
Race Equality Foundation	40	0	0
Stonewall	43	0	0
Terrence Higgins Trust	0	0	0
Total	**419**	**1**	**1**
Citizens' voice groups	**Number of hits**	**No. of relevant hits**	**Total**
Big Brother Watch	15	1	1
Citizen's Advice	0	0	0
Digital Right Ireland	10	0	0
GeneWatch	0	0	0
Healthwatch	0	0	0
Liberty	1	0	0
medConfidential	1		0
Patients Association	5	1	1
Patient Concern	No search possible. One article identified under 'Press Releases'	0	0
Total	**32**	**4**	**2**

The citizens' voice groups search produced only two relevant hits from the initial total of thirty-two (see Table 10). These were (1) a report by Big Brother Watch,[124] citing the *I v. Finland case*, which is captured and discussed elsewhere in this report, and (2) a document by The Patients Association,[125] where in one patient story the narrator commented that '*patients' notes were routinely left on the ward floor, which we feel must be a serious breach of patient confidentiality and a health issue*'.

[124]Big Brother Watch, 'Broken records: The worrying lack of security around your medical history, and how it is changing for the worse' (2010) <http://www.bigbrotherwatch.org.uk/home/2010/09/why-our-broken-records-report-matters-mk-ii.html> accessed 29 April 2014.

[125] The Patients Association, 'Stories from the present, lessons for the future' (2012) 36 <http://gallery.mailchimp.com/9dd6577cf3f36af3c2f6682ed/files/Patient_Stories_2012.pdf?utm_source=Press+List&utm_campaign=64ed66807d-Patient+Stories+Report+2012&utm_medium=email> accessed 29 April 2014.

7.A.3 Twitter Evidence

The search on Twitter resulted in 229 hits of which seventy (31%) met the criteria for evidence of an abuse of health or biomedical data (see Table 11). The 229 hits were reduced to seventy by discarding duplicate tweets on the same incident, tweets where follow-on links explaining the incident were faulty and tweets that were marketing ploys by companies offering data security services. Of the seventy relevant hits, only eleven were related to incidents in the UK. Internationally, there was one incident reported in Ireland, one in Zambia, and an overwhelming fifty-seven incidents of abuse in the US. Each incident was assigned a unique incident number, date(s) of tweet, the location of the abuse, abuse type, cause (with synopsis of the incident) and synopsis on the harm (if any evidence of harm was indicated).

Table 11: Twitter hits using advanced search

Search terms	Total hits	Relevant hits (%)
'health data breach'	1,000+	N/A
'medical data breach' excluding 'care.data'	229	70 (31%)
'biomedical data breach' excluding 'care.data'	0	0
'biological data'	0	0
'genetic data breach'	0	0
Total	**229**	**70 (31%)**

Given the vast difference in social networking website users in the US and UK, 163 million versus 32 million users respectively, and that only 15 million of the UK internet users use Twitter (versus 49 million in the US), such disparity is likely to have impacted the US-centric nature of results.[126] Furthermore, numerous US states have mandatory data breach notifications legislation,[127] making it more likely that data breaches come into the public light as opposed to the UK where no such obligation exists, except for the mandatory self-reporting of data breaches by the NHS Trusts.

Even more extreme than the hard evidence results, searches for 'biological', 'biomedical' and 'genetic' data breach uncovered zero hits. Given the informal and pseudo-social environment that is Twitter, technical terms such as biomedical, genetic or biological data (versus more broad terms such as health or medical data) will not be used with the precision one would expect in e.g. academic journals. Thus, it is likely that terminology such as biomedical, biological or genetic was too technical for the Twitter environment whereby 'health' or 'medical' was more suitable for this context. Furthermore, there is a

[126] Twitter's outgoing CEO Tony Wang announced the increase in UK Twitter users to 15 million in September 2013: <https://twitter.com/TonyW/status/375889809153462272> accessed 25 April 2014 whilst maintaining 49 million users in the US <http://www.businessinsider.com/twitter-has-a-surprisingly-small-number-of-us-users-2013-10> accessed 25 April 2014.

[127] Numerous states in the US have enacted data breach notification laws since 2002 in response to an escalating number of data breaches. California was the first such state to enact data breach notification legislation with SB 1386, Cal. Civ. Code 1798.82 and 1798.29 in 2002.

140 character limit on ‘tweets’ – biomedical and biological takes up ten characters; health six and medical seven. This could also influence the terminology used and exacerbate any preconceived notions on the conflated meanings of these terms.

7.B Typologies of abuse by cause and abuse by harm/impact

It was our intention to develop two tables – a ‘typology’ where each column represented a type of abuse (e.g. non-secure disposal, data loss, etc.), and each row either the cause of abuse (e.g. maladministration, human error etc.) or the type of impact or harm (e.g. individual distress, financial loss etc.). We then intended to note in the appropriate cells the incidents uncovered in all three evidence strands. However, the results were too complex to present in such a way, the data too large. Therefore we developed two tables each for each evidence strand – Abuse by Cause and Abuse by Harm/Impact – resulting in six tables in total.

Further, the cause was often a question of interpretation or inference in the soft evidence, and to a lesser extent in the more factually robust hard evidence. For example, when patient records were stored in a public area before being taken to a safe storage area, was this human error or maladministration or both?[(Inc39-E18)] In addition, not all categories identified in one strand had counterparts in the other two strands.

7.B.1 Hard evidence typology

7.B.1.A Inconsistent reporting across UK and European judgments

The findings from the hard evidence vary in the amount of detail given in each particular case thus influencing the amount of information that had to be deduced from what was reported. The UK case law, First-tier Tribunal (Information Rights), ECtHR and CJEU judgments were not reported according to any standardised format and thus the amount of factual and objective detail about each incident varied extensively. In all cases there was sufficient detail regarding the nature of the abuse to assign a cause for abuse (from deduction). The same analysis was undertaken when there was sufficient detail allowing inferences of harm; where there was simply no discussion of harm, this was recorded as ‘no evidence of harm’ – which again, does not indicate harm was not caused, but rather that there was insufficient reporting to infer the type or extent of harm that might have occurred.

This differs from the ICO enforcement actions such as monetary penalties, which were reported in a standardised fashion, whether in the press releases or notice forms. Thus, the ICO enforcement actions provided more consistency on the amount factual detail offered on abuse type, cause and any harm caused.

7.B.1.B Frequencies of abuse reported in the hard evidence

Table 12 represents the entirety of hard evidence categorised according to both abuse type and cause. The following discussion considers the *frequency* of abuses by the underlying cause, as ascertained from the evidence.

As shown in Table 12 below, the most prevalent cause for abuse of health or biomedical data that emerged from the hard evidence was due to 'maladministration' (ten incidents). Maladministration operated as a "catchall" cause for abuse including incidents arising from incorrect action or failure to take any action, failure to follow procedures or the law, inadequate consultation prior to taking action, broken promises in regards to the data in question etc. The incidents involving maladministration resulted most often in unauthorised disclosure or access to health or biomedical data (five incidents), or the non-secure disposal of data (four incidents) with only one incident involving the unauthorised retention of data. These incidents[128] included (for example) – in order of severity – of the abuse:

- Hospital staff disclosing sensitive personal data of patients to the press, including HIV status, despite clear procedures regarding patient confidentiality.(EUC6, EUC11)
- Improper decommissioning of hard drives, containing patient data including those that identifies HIV positive patients.(ICOM13)
- Negligent uploading of sensitive personal data of employees to a publicly accessible website, without noticing for over nineteen weeks.(ICOM10)
- Sending sensitive patient records to the wrong fax number on over forty-five occasions, compromising fifty-nine individuals' data despite clear procedures to avoid this.(ICOM14)

[128] For a full breakdown of the incidents uncovered in the hard evidence review please reference Table 23 in the Appendix.

Table 12: Hard evidence – Abuse by cause

Abuse⇨ / Cause⇩	Non-secure disposal	Loss	Technical security failing	Fabrication/ Falsification	Unauthorised		Non-use	Total by Cause
					Disclosure or access	Retention		
FOI Request					5 (IT1 ICOD1 ICOD2 ICOD3 ICOD4)			5 (10%)
To meet organisational targets				1 (UKC9)	1 (UKC1)		2 (EUC3)	2 (4%)
Involving third parties			1 (ICOM1)					1 (2%)
Facilitated by:								
Maladministration	4 (ICOM3 ICOM5 ICOM12 ICOM13)				5 (ICOM10 ICOM14 EUC6 EUC7 EUC11)	1 (EUC7)		10 **(20%)**
Human error		3 (ICOM2 ICOM6 ICOM7)			4 (ICOM4 ICOM8 ICOM9 ICOM11)			7 **(14%)**
Misinterpretation of legal obligations							1 (EUC10)	1 (2%)
Access without clinical or legitimate justification					5 (ICOP1 ICOP2 ICOP3 ICOP4 EUC8)			5 **(10%)**
Against objections or without consent of the individual					9 (UKC2 UKC4 UKC8 UKC10 UKC12 UKC13 UKC14 EUC4 EUC13)			9 **(18%)**
Insufficient safeguards					4 (UKC3 UKC5 UKC7 EUC9)			4 (8%)
Press/media					6 (UKC6 UKC11 EUC1 EUC2 EUC5 EUC12)			6 **(12%)**
Total by Abuse Type	4	3	1	1	39	1	2	**51**

The second most prevalent cause of abuse was the use of health or biomedical data against the specific wishes of the individual or without fair notice to the individual (See Table 12: Hard evidence – Abuse by cause). Each of these nine incidents involved potential or actual unauthorised access or disclosure of health or biomedical data. In many of the incidents, an individual was applying for injunctive relief to prevent the unauthorised disclosure of their sensitive personal health or biomedical data. These incidents, along with those involving *actual* disclosure or access, were considered together due to the similarity of issues encountered in such cases. Examples, in order of severity, include incidents where injunctions were sought in order to *prevent* unauthorised disclosure to incidents, whereby the data were in fact disclosed:

- An injunction was applied for when an abusive husband asked to see the psychiatrist, psychologist and therapist records of his wife and children (despite their objections.(UKC12)

- The disclosure of prescription data to a pharmaceutical company without disclosure to patients of this proposed use. (UKC14)

- Individuals' next-of-kin were not notified of the use of patient records and tissue in a public inquiry.(UKC2)

- A claimant applied for access to a third party's confidential medical and personnel records (despite the third party's objections) for his court proceedings against his employer.(UKC8)

- A health authority seeking disclosure of medical records in order to carry out an investigation into e.g. the possible over dispensing of medicines, when patient consent was refused or not obtained.(UKC13)

As show in Table 12, the third most prevalent cause was human error (seven incidents). Human error resulted in either the loss (three incidents) or the unauthorised disclosure or access of data (four incidents). Incidents identified as being caused by human error, in order of severity[129] include:

- A social worker left sensitive documents in a plastic shopping bag on a train including GP and police reports relating to cases of sexual abuse and neglect, whilst working on them during a commute between home and work.(ICOM7)

[129]Here we reference the spectrum of *causes* of abuse and of *harm* provided in Section 4.B *Causes for abuse*, Section 4.C *Harm types*, Figure 5 and Figure 6.

- A social worked used a previous case as a template, but sent a copy of the old report (instead of the new one) to the wrong person, revealing sensitive personal data including details of an alleged criminal offence and physical and mental health to the wrong person.(ICOM8)

- Relating to a nurse's misconduct hearing, three unencrypted DVDs containing sensitive information regarding children were lost in transit.(ICOM6)

- The loss of an unencrypted USB memory disk on the premises of a local authority.(ICOM2)

The fourth most prevalent cause of abuse[130] featuring in five incidents was unauthorised access without clinical or otherwise legitimate justification (See Table 12). It is worthwhile noting that the three incidents, all occurring in the UK, were criminally prosecuted. These incidents were prosecuted by the ICO on the basis of breaching section 55 of the DPA. Section 55 makes it an offence if a person *knowingly* or *recklessly*, *without the consent* of the data controller, obtains, discloses or sells personal data or the information contained in personal data, or procures the disclosure to another person of the information contained in personal data. These incidents are distinguished from the other non-intentional or negligent cases (e.g. human error or maladministration), given the wilful and intentional nature that motivated the guilty party to abuse the data. ***This more wilful and intentional breach of data protection law featured less than other more non-intentional abuses, representing only 8% of total incidents identified in the hard evidence.***

These incidents included (for example) in order of severity:

- A manager of a health service accessed the health data of over 2,000 people in order to use the data to set up a new fitness company. (ICOP2)

- A receptionist at a GP's practice obtained sensitive medical information relating to her ex-husband's new wife unlawfully. (ICOP3)

- A health worker obtained the patient data of five members of her ex-husband's family in order to obtain their new phone numbers. (ICOP4)

7.B.1.C Incidence of abuse involving DNA profiles and tissue

As stated above, only one incident was identified during the evidence review involving 'genetic data'. This incident related to the (potential) harms arising out of the *indefinite* retention of DNA profiles by UK authorities. (EUC7) Given the important implications raised by

[130] Tied with unauthorised disclosures arising from FoI requests, also five incidents.

genetic data, we discuss this incident in further depth in Section 9.A.7. Further we consider a focused review on genetic data as an area warranting further and future research (see Section 10.D).

7.B.1.D Frequencies of abuse by harm reported in the hard evidence

As shown in Table 13 below, a single incident could cause multiple forms of harm. However, the single most prevalent 'harm' uncovered was not actual harm, but the ***potential for harm*** as perceived by the adjudicating body (i.e. court, tribunal or ICO). Potential harm was found in an overwhelming 53% (or twenty-seven incidents). Within the spectrum of *actual* harm,[131] emotional or physical, individual distress was most prevalent with 18 incidents (35%). However the spectrum of *actual* harm was wide-ranging and included not only individual distress, but also the receipt of suboptimal clinical care, financial loss and harm caused to broader public interests (e.g. cases of reputational damage to public organisations such as the NHS or damage to the public trust in the confidentiality of the health profession). We also recorded incidents if there was no discussion of harm at all,[132] or if there was an explicit finding of *no* harm, as these both could reflect the narrowness of harm provided for in the legal regime as opposed to broader conceptions of *impact* revealed in the soft evidence.

[131] Which as discussed previously, was not intended to be exhaustive but reflective of the actual evidence uncovered. There are many other types of harm that could befall an individual, an organisation or negatively impact broader public interests. The typologies of abuse by harm/impact merely reflect the evidence base produced during this exercise.

[132] Reflecting our findings of 'no evidence of harm', which does not mean *no* harm occurred, but rather that there was insufficient detail reported to categorise the extent of and/or type of harm that might have occurred.

Table 13: Hard evidence – Abuse by harm

Abuse⇨ / Impact⇩	Non-use	Non-secure disposal	Technical security failing	Loss	Fabrication/Falsification	Unauthorised		Total
						Disclosure or access	Retention	
Individual distress	1 (EUC3)					15 (UKC1 UKC6 ICOP2 ICOP3 ICOP4 ICOM8 EUC1* EUC2 EUC4 EUC5* EUC6 EUC8* EUC9 EUC11* EUC12 EUC14)	1 (EUC7)	**18 (35%)**
Suboptimal clinical care						2 (EUC8* EUC11*)		**2 (4%)**
Financial Loss						2 (EUC5* EUC14*)		**2 (4%)**
No evidence of harm	1 (EUC10)					4 (UKC2 UKC13 ICOP1 EUC13)		**5 (10%)**
***Potential* for harm**		4 (ICOM3 ICOM5 ICOM12 ICOM13)	1 (ICOM1)	3 (ICOM2 ICOM6 ICOM7)	1 (UKC9*)	19 (UKC3 UKC4 UKC7 UKC8 UKC10 UKC11 UKC12 IT1 ICOM4 ICOM9 ICOM10 ICOM11 ICOM14 ICOD1 ICOD2 ICOD3 ICOD4 EUC1*)		**27 (53%)**
***No* harm found**						1 (UKC14)		**1 (2%)**
Damage to broader public interests					1 (UKC9*)	1 (UKC5)		**2 (4%)**
Total Incidents								**51**

*** Indicates an incident resulted in more than one type of harm, thus the percentages versus total incidents (51) do not tally.**

7.B.1.E Potential harm

The most prevalent type of harm found in the hard evidence was the ***potential*** for harm. The adjudicating body inferred harm, whether it was a UK Court, the ICO (and less often the ECtHR or CJEU), based on the nature or severity of the type and cause of abuse. In incidents categorised with 'potential harm', there was not necessarily evidence of *actual* distress, either emotional or physical. Thus, harm was inferred in cases such as:

- A further monetary penalty notice was issued by the ICO in relation to the improper decommissioning of hard drives of NHS Trusts, which contained health data regarding HIV-positive patients. Since not all of the hard drives were recovered, and because the data was extremely sensitive, it was considered likely that the data could be abused in future to discriminate against the individuals implicated or otherwise cause harm. (ICOM13)

- The High Court of Justice in England and Wales found against the disclosure of confidential expert testimony and reports from a psychiatrist in a family law case (where disclosure was against an abused wife's wishes) in part, because '…the disclosure of such personal material would be likely to cause the mother distress and upset which would be highly likely to impact adversely upon a child living in the same household.' (UKC3)

- When a USB stick was lost on the premises of North East Lincolnshire Council, the ICO considered in its issuance of a monetary penalty the risk assessment taken post-breach, which indicated '…that the loss of the sensitive personal data is likely to lead to the ill health of those affected through the disclosure of the data or due to a break in the services, which they were receiving. The likely damage and distress to the data subjects is substantial due to the volume of data which has been lost, and that the data subjects are children aged 5 - 16, some of whom are deemed vulnerable (and their families).'(ICOM2)

- In the landmark case *Campbell v MGN Ltd* [2004] UKHL 22, the House of Lords inferred that Ms Campbell *would* be distressed since '…[a] person in her position would find disclosure highly offensive, and might also be deterred from continuing with the therapy, thereby causing a setback to recovery.'(UKC11)

- When the ICO issued a monetary penalty notice to the Central London Community Healthcare NHS Trust for incorrectly faxing the sensitive personal health data of patients on over forty-five occasions, the ICO inferred individual distress of those individuals whose data were compromised as it was 'likely to cause substantial distress to the patients'; although no complaints were received from data subjects.(ICOM14)

7.B.1.F Findings of actual harm

Notwithstanding, *actual* harm in the form of individual distress was found in cases where complaints were made by the individuals implicated (signalling their distress), or when the courts otherwise found sufficient evidence of *actual* harm[133] by individual distress. These cases included:

- In the ICO's prosecution of a former health service manager based at a council-run leisure centre. The council received complaints of distressed patients who were approached by the former manager who unlawfully obtained their sensitive medical information to use the data for a new fitness company he was setting up.(ICOP2)

- The ICO's prosecution of a former receptionist of a GP office who was unlawfully obtaining sensitive medical information relating to her ex-husband's new wife. The receptionist had sent a text message to her ex-husband's wife referring to the latter's highly sensitive medical information taken from her medical record. The ICO received evidence of this harassment and the distress caused to the ex-husband's new wife.(ICOP3)

- The ECtHR found evidence of 'great personal distress' caused to both the Countess and Earl of Spencer by virtue of the strain caused to their relationship and to the medical treatment for Countess Spencer's mental health and bulimia.(EUC2)

- The ECtHR found ample evidence of individual distress upon the publication of information about the applicant's husband's HIV-positive status and his extramarital affair with a woman living with AIDS, an affair that produced two children. Specifically, '[t]he newspaper article had humiliated the husband and the publication of information about his private life had caused him non-pecuniary damage, had an impact on his health, and a negative influence on his family life and his reputation as well as restricting his family's opportunities to interact with others. He died and his wife brought suit based on such harms.'(EUC5)

The other types of harms – namely suboptimal clinical care and financial loss – also produced evidence of 'actual' harm including:

- In reference to the final case of actual, individual distress above, the deceased had to move from their village and lost his job due to the publishing of an article about his HIV-positive status and extramarital affair and children with a woman living with AIDS.(EUC5)

[133] Actual harm as defined and legally recognised in the law – see Section 3 above for further explanation on the narrow, regulatory notion of harm.

- A young woman had become pregnant after being brutally raped, and when seeking an abortion the hospital issued a press release regarding her situation causing the young woman to be subject to a national news frenzy – she eventually was forced to leave that hospital and seek an abortion 500km from home.(EUC11)

7.B.1.E Findings of 'no' harm or where there was 'no evidence of harm'

In contrast, two categories on the spectrum of harm involve findings of *no* harm or cases where harm was not considered at all by the adjudicating body. Only one incident was uncovered where the court categorically stated there was *no* harm.(UKC14) Of the hard evidence results, the third most prevalent were cases where harm was simply not discussed (five incidents).[134] For incidents where harm was simply not discussed by the adjudicating body ('no evidence of harm'), the cases would typically state the facts surrounding the breach and/or fines imposed, without discussing harm:

- That the processing of health or biomedical data was against patient wishes (consent not provided) or no response.(UKC2)
- The amount of fines that were paid.(ICOP1)

7.B.1.F Harm arising from non-use of data

As only two cases of non-use of health or biomedical data emerged from the results this warrants separate discussion – in one case, harm was also not discussed.(EUC10)

In *Gillberg v Sweden*(EUC10) the discussion focused on the interference with the human rights of the individuals who wanted access to the research data in question (which involved children's health data). Whereas all other cases where human rights were engaged by way of Article 8 (private and family life), the human rights engaged for *non-use* of data included: (1) the claimants' rights to freedom of expression (Article 10) as it related to their perceived *right* to *access* the health (research) data in question, and (2) the claimants' Article 6 rights (which protects an individuals rights to a fair trial) to have the ECtHR judgment implemented as it ruled in favour of granting access to the health (research) data.

The only other cases that involved an incident of *non-use* was the ECtHR case, *McGinley and another v United Kingdom*.(EUC3) This case dealt with the non-disclosure of data regarding the radiation exposure levels to former members of the armed services who were stationed near the site of nuclear tests on or near Christmas Island in 1958. The UK would neither confirm nor deny the existence of such documents despite the contentions of the applicants. The Court considered the issue of *non*-disclosure (or thus non-use of the data) in terms of its capacity to ease individual distress caused by the fear of potential damage caused by being near the nuclear blast – in this regard, the non-disclosure of documents was considered sufficiently linked to the applicants' private lives to engage

[134] And categorised as 'no evidence of harm'.

Article 8. Whilst Article 8 was engaged, the applicants' claim ultimately failed because they had not exhausted administrative procedures to request the data under Freedom of Information legislation in the UK.[135]

Importantly, both cases of non-use were considered to engage the human rights of individuals. This in part recognises the 'harm' that can be caused when data are *not* used, and thus the value in searching for examples of such harm – albeit with meagre returns – as it relates to failures to use data. Given the lack of evidence uncovered on *non*-use of data, we dedicate fuller discussion to the implications arising out of non-use in Section 9.A.8 below.

7.B.1.G Harm to broader public interests

Finally and considered separately are incidents not involving *individual* harm, but harms to broader public interests involving damage to a public institution's reputation or diminished confidence in the doctor-patient relationship etc. Despite the fact that the law does not explicitly recognise harms to the public interest as they might arise for individuals, the hard evidence search *did* identify five incidents, where the adjudicating body considered harms or potential harms to broader public interests. These incidents included, for example:

- Damage to the confidential nature of police interaction with their Occupational Health and Welfare department if information imparted during such interactions were disclosed without '…any reference or notice to the applicant, without affording him reasons for the decision or an opportunity to have made representations before or during the decision making process.'(UKC5)

- In a libel action against the BBC for publishing a story on NHS hospitals falsifying waiting times, the Court considered the falsification of waiting times as damaging to the public interest. In particular, the case was considered important given that '…institutional corruption within a public body…has gone unpunished[136].(UKC9)

- The ECtHR found *potential* for harm to broader public interests, including the creation of a possible disincentive for other HIV-positive patients to seek appropriate treatment but also to the 'the interests of a patient and the community as a whole in protecting the confidentiality of medical data'[137].(EUC1)

[135] *McGinley and another v United Kingdom*(EUC3) raises interesting questions regarding the linkage of occupational health records with mainstream, medical records such as those held by the NHS. The armed forces are a special case, as they hold their own records whilst personnel are serving – it is unclear on the extent to which such records are shared or linked when a) a civilian joins the armed forced and b) when personnel leaves the service.
[136] Further discussion on incidents of falsification and fabrication of data will be provided in Section 9.A.6 Falsification and fabrication below.
[137] *Z v Finland*, paras [96]-[97].

It was expected that less evidence would be found on harms caused from 1) non-use of data, and 2) harm caused to broader public interests, given the narrow conception of harm in the law. There are no legally recognised *positive* obligations to use health or biomedical data, in any particular way, bar a patient's request for access to their *own* health records.[138]

Summary of hard evidence results

The hard evidence uncovered unauthorised disclosures and access to health or biomedical data as the most prevalent ***abuse type***, followed by non-secure disposal of data, data loss, *non*-use of data, unauthorised data retention and technical security failures. Maladministration was the greatest ***cause for abuse***, whereas only four incidents or 8% of the evidence represented criminally punishable (intentional) abuses of health or biomedical data. Although the law will provide compensation only for *actual* harm, the hard evidence did uncover instances of the courts and ICO considering *potential* harm in an overwhelming 53% of the hard evidence. Thus, evidence of *actual* harm featured less prominently in the hard evidence, with incidents of individual distress as the most prevalent form of *actual* harm caused (35% of the evidence). Surprisingly, despite the lack of recognition for harms caused to the public interest in legislation, the courts did consider and find actual harm to such public interests. And relatedly, although no positive obligations exist to *use* health or biomedical data (bar FOI obligations), the ECtHR considered non-use of data as engaging human rights which may have implications for wider uses of health or biomedical data, such as in research.

[138] However, in depth consideration of the role or impact of Freedom of Information legislation in this regard is outwith the scope of this report.

7.B.2 Soft evidence typology

Whereas it was possible to present the same abuse type, cause and impact categories for the hard evidence and for Twitter, this was not the case for the soft evidence. Please note the following provisos.

- In contrast to the hard evidence, the newspaper figures presented are based on our interpretations of their sometimes-sparse detail, that is, some did not provide statements rigorous enough to use more differential categories with good conscience. For example, erring on this side of caution, there was a large cluster of cases involving 'maladministration', whereas some of these could also have been 'human error' or 'human error' only.
- Further, a newspaper article could refer to cases involving multiple causes (e.g. 'theft' and 'loss'), and such articles appear in the tables more than once.
- Finally, every attempt was made to ensure that all articles were assigned to one incident only, and that each soft incident was unique. Those incidents that might not have been unique were discounted.[139]

7.B.2.A Abuse by cause typology

7.B.2.A.1 Incidents involving NHS Staff

In Table 14 it can be seen that forty-eight incidents involved NHS staff (or, in the case of theft, premises). The first most common abuse type was unauthorised data access or disclosure; such abuse accounted for one in three (14; 29%) incidents. For example:

- A constituent requested his Welsh Assembly Member to investigate why third parties are in receipt of medical records. Here, records sent to the DWP and ATOS were being opened routinely by Royal Mail staff.(news14) In the words of the constituent, '*People are sending very personal information and I have a right to know this is happening: I feel like I've been misled*.'
- As investigated by the ICO, Torbay Care Trust made details on a spreadsheet of staff available on the Internet in error.(news15) Details included sexual orientation and NI numbers. The error was reported by a member of the public, and it was estimated that the spreadsheet had been viewed 300 times before being reported.

[139] We exclude newspaper incidents news45, news48, news54-59.

Table 14: Soft evidence: Abuse by cause

Cause ⇩ / Abuse ⇨	Non-secure disposal	Loss	Theft	Fabrication/ falsification	S/W failing	Unauthorised data		Other	Total
						disclosure or access	retention		
Involving NHS staff (or premises):	6 (**13%**) (news8,10,11,18, 29,42)	7 (**15%**) (news6,12,13,1 7,26,31,44)	5 (**10%**) (news17,31,34, 40,52)	6 (**13%**) (news2,3,4,5,9, 35)	3 (**6%**) (news1,13,35)	14 (**29%**) (news14,15,16,19,23,24,25 ,30,32,33,39,43,47,50)	2 (**4%**) (news7,49)	4 (10**%**) (news27[140],2 8[141],51[142],53 [143]news60[144])	**48**
To meet NHS targets				3 (news2,3,5)					
To protect professional reputation				2 (news4,35)	1 (news35)				
For self-gain (curiosity, financial gain)						3 (news23,24,32)			
Not involving NHS staff	2 (news18,38)					9 (news14,20,21,22,30,33,37 ,46,50)			**11**
Facilitated by:									
Maladministration	7 (**16%**) (news8,10,11,18, 29,38,42)	5 (**11%**) (news6,13,17,2 6,31)	5 (**11%**) (news17,31,34,4 0,52)	6 (**13%**) (news2,3,4,5,9, 35)	3 (**7%**) (news1,13,35)	15 (**33%**) (news14,15,20,21,23,24,25 ,30,32,33,37,39,43,47,50)		4 (9**%**) (news27,28,5 1,news60)	**45**
Human error		2 (news6,12)				4 (news16,19,22,33)		1 (news51)	
Misinterpretation of legal obligations							2 (news7,49)		

[140] Data destroyed in error.
[141] Survey data sent to deceased patients.
[142] Incorrect coding.
[143] Sale of data to Actuarial Society.
[144] Extremely poor record keeping at GP surgery.

- Three incidents involved the use of social media.[news25,news43,news47] All three reached the media through FoI requests (the Guardian Healthcare Network, Scottish Conservatives, Big Brother Watch resp.). In response to the Guardian Healthcare Network's request, which uncovered figures across twenty-five Trusts, Andy Jaeger, Assistant Director of Public and Professional Communications at the NMC said

'[S]taff *misuse of social media is largely unintentional, but there are cases that the NMC deals with which are "absolutely deliberate" – which is perhaps not surprising given that the regulator deals with referrals relating to nurses and midwives that may not be fit to practice. Such instances include pursuit of relationships with patients and bullying and harassment of colleagues.'*

The second most common abuse types were loss (7; 15%), followed by non-secure disposal and fabrication/falsification (6; 13% each), and then theft (5; 10%). 'Other' incidents are explained in footnotes to Table 14. Incidents of loss could sometimes be explained by a perhaps understandable thoughtlessness against the backdrop of extreme workloads of NHS staff, coupled with a lack of staff awareness training.

- As investigated by the ICO, a consultant psychiatrist lost data, including notes on a patient's mental health tribunal, that was not secured properly to his bicycle.[news6] The ICO concluded that insufficient steps had been taken by Cardiff and Vale Health Board to make employees aware of the fact that they could indeed access the network remotely.

Other losses had far more serious consequences. For example:

- At Imperial College Healthcare NHS Trust, it was estimated that thousands of patient medical records were lost, caused by software problems and staff IT errors.[news13] Crucially, these included patients awaiting cancer test results, and of those affected by the loss, seventy-four died. The Trust claims that no one died because of waiting for results or care. The external reviewer, Terry Hanafin, concluded that this was a '*serious management error'*.

Although one would expect to see fewer and fewer reported incidents of loss over time, one article showed that this is not necessarily the case.

- In 2014 a FoI request by the Scottish Liberal Democrats ascertained that there were 806 incidents of data loss across Scottish Health Boards in the previous five years.[news41] Whereas there were eighty-six losses in 2009, the number of loss increased to 223 in 2013.

Incidents of non-secure disposal were all known to the ICO with the exception of:

- British Telecom led a 5-country study together with the University of Glamorgan, in which three hundred hard drives were bought at auction.(news38) According to *The Sun* newspaper, one third of the drives contained sensitive details including NHS patient notes. Investigating this short tabloid report further, we found that three hundred and seventeen drives were purchased in the UK, Australia, Germany and the US.[145] However and as noted in *Techworld*, 'of the countries surveyed, the UK did relatively well by the admittedly low standards of data security uncovered'.[146]

Incidents of theft all pre-dated 2012. This is encouraging, in that it suggests that theft of hardware is becoming a thing of the past.

The six Incidents of falsification/fabrication were considered severe. For this reason, all are reported below:

- One incident involved the Bristol Royal Hospital that in 2002 was embroiled in a scandal of such proportions that an inquiry ensued. The article here is from 2014, demonstrating how long the process can be to see justice (potentially) being served.(news2) Bereaved parents noted that the hospital had failed to declare the death of their son, possibly to provide better figures for National Institute for Cardiovascular Outcomes Research's league tables. Sir Bruce Keough has now ordered lawyer-lead inquiry into the children's' Ward 32.
- Also in 2014, the National Audit Office identified in NHS England (Leeds, Oxford, Colchester, North West London Hospitals Trust, Barnet & Chase Farm Hospitals) that only 43% of cases were recorded properly.(news3) Twenty-six per cent of cases showed falsified waiting times, and thirty-one per cent of incomplete record keeping.
- In 2013 two paramedics employed by the Welsh Ambulance Trust were struck off, after one failed to assess a thirty-year-old patient, resulting in her death.(news4) Both paramedics were party to falsifying the data.
- In 2013 several articles emerged about the Colchester University Hospital scandal.(news5) The sources for the articles were inquest and *Monitor*, the Trust Watchdog. Cancer records were being falsified to meet national cancer targets, and of sixty-one cases reviewed, twenty-two showed that patients had been placed at risk of receiving care that was unsafe or not effective. Management failed to investigate allegations and concerns raised by staff; rather, staff were bullied into silence.
- In 2013 it emerged that the Care Quality Commission reverted possibly to cover-up tactics to conceal severe shortcomings at Furness General Hospital.(news9) It

[145] Andrew Jones et al, 'The 2006 analysis of information remaining on disks offered for sale on the second hand market' (2006) 1:3 Journal of Digital Forensics, Security and Law.
[146] John Dunn 'Hard disks still scrapped with data intact: Simple forensics reveal secrets, says study' (2006) <http://news.techworld.com/security/6618/hard-disks-still-scrapped-with-data-intact/> accessed 29 April 2014.

transpired that information on the scandal (where, for example, sixteen babies had died) was forwarded but with names of responsible individuals redacted. It took the intervention of the ICO and Health Secretary, Jeremy Hunt, to rectify this.

- It emerged at a Coroner's inquiry in 2009 that a nurse had falsified a patient's record at Holloway Prison.(news35) She had failed to administer psychopharmaca to the prisoner, who went on to complete suicide, and then she altered the patient's record on the EMIS system. An audit revealed that no such medication had been administered on the day of the suicide. Note, as well as classifying this article under falsification/fabrication, it is also classified under a software failing. However, this is not as clear-cut as one would hope. On the one hand, it was the rigor of the audit that allowed the falsely amended patient record to come to light. On the other hand, the record was amended falsely because EMIS allowed this.

7.B.2.A.2 The motivations behind the incidents involving NHS Staff

Overall, we were able to ascertain the motivations behind nine incidents. As shown in Table 15 three were to meet NHS targets, two to protect professional reputation, and three for self-gain. The incidents not discussed thus far are the three pertaining to self-gain.

Table 15: Determinable motivations behind all incidents involving NHS Staff

	Fabrication/falsification	S/W failing	Unauthorised data disclosure or access
To meet NHS targets	**news2**-Bristol Royal Hospital **news3**-NHS England **news4**-Colchester University Hospital		
To protect professional reputation	**news4**-Colchester University Hospital **news35**-Holloway Prison	**news35**-Holloway Prison	
For self-gain			**news23**-Royal Victoria Hospital **news24**-Edinburgh Royal Hospital **news32**-Moregate Primary Care Centre

- As investigated by NHS Tayside and the NMC, a nurse at the Royal Victoria Hospital accessed ten medical records.(news23) She was sacked and struck off. It is unclear what her motivations were, but it is reasonable to assume self-gain, because she had accessed friends' records. We cannot judge whether this was done with misplaced benevolence, malevolence or idle curiosity.
- The case at Edinburgh Royal Hospital involved a cleaner who obtained a female patient's details and then contacted her, presumably out of romantic/sexual interest.(news24) It could be that the details were from the patient's records, but the hospital maintains that the information was taken from a floor plan of A&E displayed on a screen. The patient's name alone would have been sufficient, because the cleaner tracked her down via Facebook. The experience left her feeling vulnerable: '*I*

didn't know who he was, what he was capable of. I didn't know if he was just going to turn up at the house. It's just wrong.'

- Incident 32 (news32) involved a nurse at Moorgate Primary Care Centre who gave patients' details to her boyfriend, employed by company handling personal injury claims, Direct Assist, in Bury. We have no knowledge of any impact her actions may have had on the subjects. She was sacked, and in the run-up to her court case, she stabbed her daughter fatally and made an uncompleted suicide attempt. She is currently serving a twelve-year custodial sentence for manslaughter on the grounds of diminished responsibility.

7.B.2.A.3 Incidents involving individuals outside of the NHS

Also shown in Table 14, eleven breaches involved individuals outside of the NHS (but possibly also NHS staff). Two cases involved non-secure disposal. For example, hard-drives were handed over to a sub-contractor by Brighton and Sussex University Hospitals NHS Trust.(news18) He failed to decommission them before sale on eBay.

The other nine cases involved unauthorised data disclosure or access, five within the UK and four abroad. Examples in the UK include:

- The hacking incident was reported where James Jeffery stole 10,000 records from the British Pregnancy Advisory Service's website in 2012.(news20) According to *The Independent*, since his conviction there have been a further 2,500 attempts to hack into this site, in a third of the cases from North America and from Russia.
- Based on a FoI request in 2012 by Channel 4's *Dispatches* programme, there were approximately five cases daily where a staff member at the DWP sought to access or to disclose data without authorisation.(news46) The request revealed only eleven 'serious cases'.

Examples abroad include:

- The NHS technology supplier, GE Healthcare, sent 600,000 records to the US by mistake.(news21) The incident was reported only a year later. It was reported in *The Sun*, and no further details were available.
- In 2009 the ICO started to investigate why data from private hospitals were being sold to individuals with access to IT companies in India, allegedly for 'transcription purposes'.(news37) According to the *Daily Mail*, the purchasers were undercover investigators. What seems to be clear is that the private clinics' records did include NHS records, but none had sent material directly for transcription abroad. The first service supplier was *DGL Information Technologies UK*, who sub-contracted to *Scanning and Data Solutions*, who in turn worked with subcontractors, one of whom was located in Pune, India.

7.B.2.A.4 Breaches facilitated by maladministration or human error – borderline cases

Forty-five news incidents (Table 14) involved maladministration, and 33% (fifteen) of these were due to unauthorised disclosure or access. However and as noted earlier, this figure is likely inflated, because it was often not possible to ascertain any element of human error. Indeed, only seven incidents were clearly human error. It is also questionable to what degree 'maladministration' identified here would also be deemed to be such in the hard evidence. For these reasons, we do not comment on this section of the table.

7.B.2.B Abuse by Impact typology

The next question is whether and to what degree has a harm caused by an abuse impacted upon the individual, the institution or on broader society?

- At the individual level, we found only one incident that had the potential to cause financial harm. In 2014, it became known that the HSCIC predecessor, NHS IT, had sold 47m patient records to the Staple Inn Actuarial Society for £2,200.(news53) According to an HSCIC spokeswoman, '[t]he HSCIC believes greater scrutiny should have been applied by our predecessor body prior to an instance where data was shared with an actuarial society'. However, as a result, the premium for critical illness cover for those aged under 50 has increased.[147] Although this could be seen as an increased financial burden on the insured individuals, this premium rise can be considered as appropriate and informed.
- We found no evidence of abuse that impacted upon institutions outside of the NHS, and negative impacts on the NHS could only be presumed (e.g. loss of public trust and confidence).[148]
- In cases where the NHS had (inadvertently) provided data to third parties, our reading of the respective articles indicated that no blame was attributed to these third parties.
- We also found no direct references to societal harm.

The impact of identified harms reported here, therefore, relate only to the individual (see Table 16). In the fifty-seven incidents, thirty-four (60%) had no reference to the impact of a harm upon the individual. Of those that did, some indicated multiple impacts. Ten (18%) referred to distress, one (2%) to reputational damage, eight (14%) to suboptimal clinical care and three (5%) to a *potential* for an impact of harm.

[147] Indeed, this was the precursor to the debate surrounding care.data.
[148] However, the recent public outcry over care.data would seem to indicate that tangible harm is not needed in order to evidence a compromise in trust between individuals and public institutions such as the NHS, which arguably negatively impacts the public interest.

Table 16: Soft evidence: Abuse by impact

Abuse⇨ / Impact⇩	Non-secure disposal	Loss	Theft	Fabrication/ falsification	S/W failing	Unauthorised		Other	Total
						disclosure or access	retention		
Individual distress				4 (news2,3,5,9)		3 (news14,16, 37)	1 (news49)	2 (news51+G8,news60) (human error)	**10 (18%)**
Damage to individual reputation								1 (news51)(human error)	**1 (2%)**
Suboptimal clinical care*		1 (news13*)		5 (news2,3*,4*, 5*,9*)	2 (news1,13*)				**8 (14%)**
Financial Loss								2 (news53,~~Ma05~~) (data sold comm. purposes, ~~legal costs~~)	**1 (2%)**
No discussion of individual harm	7 (**20%**) (news8,10,1 1,18,29,38, 42)	7 (**24%**) (news6,12,1 7,26,31,41, 44)	6 (**17%**) (news17,31, 32,34,40, 52)	1 (**3%**) (news35)	1 (**3%**) (news35)	12 (**34%**) (news15,19,21 ,22,23,30,33,3 9,43,46, 47,50)			**34 (60%)**
***Potential* for harm**						2 (news20,25)		1 (news28) (human error?)	**3 (5%)**
								Total	**57**

* Suboptimal care that led to or possibly led to death and *News3 and news5 involve Colchester Hospital

Identifying incidents of actual harm are central to this report. Therefore we draw here on two tables. The Abuse by Impact Table 4 should be regarded as an orientation only, simultaneously giving an overview of the findings. Later we present those incidents where we can also report subjects' statements regarding the harm they have experienced (see Table 26 in the Appendix).

Of those presented here, ten were made by the subject or their next-of-kin and six by citizens' voice groups. For each incident, we cite in brackets the news-number, followed by the newspaper where the citations appeared, for example, (news28/S06).

7.B.2.B.1 Impact of harm caused through falsification/fabrication

These were severe instances of abuse, where the NHS organisation(s) suffered reputational damage and a great loss of public trust. These are instances of lives at risk, or indeed lives lost. In the three following incidents, note that the subjects became socially and politically active, and sought justice.

- Bristol Royal Hospital failed to declare the death of a child, and the parents '*believe Trust chiefs "covered up deaths and blatantly lied*"'.(news2/Mi02)

- In the wake of the CQC cover-up at Furness General Hospital, bereaved father James Titcombe had led the campaign for a public inquiry into '*serious systemic failures'* … and called reports of a cover-up at the Care Quality Commission '*shocking. … It embodies everything wrong with the culture in the NHS*'.(news9/B03)

- In the wake of the Colchester University Hospital scandal, (news5/Te11) the bereaved mother of a four-year-old who died after delays in treatment '*called for "justice" for her son, and said no-one at the NHS trust had been held accountable for the failings, or even disciplined'.* Going public is pro-active coping strategy, and documents again a subject's need for restorative justice.

Also in the wake of the Colchester University Hospital scandal, (news5/Te11) we see another type of reaction, here one that demonstrates understandable despair and hopelessness at the time of the event.

- A widow 'said she was left "crying down the phone" to medical staff, pleading for them to treat her husband.' This is admittedly scant evidence, but against the backdrop of the Colchester scandal and the number of patients who were misdiagnosed or where diagnosis was so late that cancers were now terminal, the impact statement could reveal not only what is clearly poor treatment or lack thereof, but also a case resulting from the fiddling of waiting lists. The main point here is that the (indirect) impact of falsification can leave the subject or loved one so disempowered, that the event can lead to long-term trauma. The consequences of such events on the bereaved are

well-documented and can have year-long negative implications for mental health (see for example Carr, 2003).[149]

7.B.2.B.2 Impact of harm caused through human error

Human error can and will occur. Errors can include miscoding, failure to update records in a timely manner and misfiling. Further, the impact of the error can affect one individual only or a group of individuals. The incident below had the potential to impact upon the loved ones of 903 deceased individuals.

- In 2011, the Scottish Government sent the Inpatient Patient Experience survey to 903 deceased patients.(news28/S06) As reported in *The Sun*, Margaret Watt of the *Scotland Patients Association*, '*branded the blunder "outrageous" and said grieving families deserved an apology. She said: "Someone should take a fall for this because it is absolutely shocking. It is unforgivable and I hope they extend an unreserved apology.*"'

The next incident was probably due to misfiling of one note in a patient's record. Although the GP surgery admitted to its error, it was not willing to amend the record until it lost its case in court.

- Reported in 2010, a patient was erroneously labelled an alcoholic in her patient record at her GP surgery.(news51/Ma22) Helen Wilkinson fought to have her record amended, but whilst the surgery was sympathetic, it was not willing to comply with her wishes. She took the surgery to court, drawing on the DPA and arguing that the NHS had caused her 'unwarranted and substantial distress'. The surgery then amended her record. Reporting later about the incident and its impact in *The Guardian* in 2006,(G26) Ms Wilkinson said *'I went ballistic. To be labelled an alcoholic – who had seen it? Who knows, literally hundreds could have seen it'* and rightly wondered how such false information could be used, for example, if the subject were someone in the middle of a 'messy divorce'. The incident was so distressing for Ms Wilkinson that she has since withdrawn from the NHS.

Finally, this distressing incident suggests far more than the mere misfiling of a piece of patient information. It documents record keeping standards of the poorest kind.

- Mary Kerswell, a former biomedical scientist, was asked by her GP surgery, Biggleswade Health Centre in 2013, to undergo a urine test for a kidney condition she did not have.(news60) Concerned, she requested a copy of her patient notes, but these were not available at the surgery at the agreed time. She felt that something was amiss, so refused to leave. The police were called and she was arrested. Receiving

[149] Deborah Carr, 'A "good death" for whom? Quality of a spouse's death and psychological distress among older widowed persons' (2003) 44:2 Journal of Health and Social Behavior 215-232.

the notes three months later, she found that her notes revealed incorrectly that she had chronic kidney disease, was a heavy smoker, lived with Alzheimer's, had a hysterectomy and a double hip replacement. *'I was utterly shocked … it read like a post-mortem, it really did. … It could have been really dangerous. Who knows what implications these errors could have had if I'd been taken to hospital in an emergency?'*

7.B.2.B.3 Impact of harm caused by unauthorised/inappropriate disclosure or retention

Subjects' statements have been addressed above concerning the female who was contacted by a hospital cleaner (news24/S05) and Royal Mail staff opening letters containing medical details to ATOS and DWP.(news14/In05) Three other incidents came to light. The first two express the subjects' outrage at the affront on their privacy. The third was distressed because of the potential for causing her mother distress.

- Commenting on the fact that data had been sold illegally to undercover investigators in 2009, one patient commented *'But this is our life – this is your flesh and bones you're talking about. It's just one step away from grave robbing)'*.(news37/Ma6)
- In 2010, it emerged that Guthrie cards with babies' blood samples were being retained by hospitals in the UK.(news49/ti12) Further, coroners and the police were allowed to access these. In the words of Shami Chakrabarti, (also member of *Liberty*): *'"As someone who gave consent for my own baby to be tested, I'm horrified that anyone would breach my trust, keep my child's sample for years on end and use it for all sorts of extraneous purposes."' GeneWatch* also noted that '"*Giving mothers a leaflet does not amount to informed consent. No one who has just given birth is in a state to understand the full implications of how their baby's genome might be used in future*."'
- In 2012 it was reported that Caseway Hospital, part of Northern Trust, had sent eight patient letters to the incorrect recipient.(news16/B08) This was extremely distressing for one affected female, because '*This is a complete shock, I know nothing about it … I did [undergo the test], but nobody knows that. All that I got done, I hid that from my mother. She knows nothing about anything*.'

7.B.3 Twitter evidence typology

7.B.3.A Frequencies of abuse reported in the Twitter evidence

As stated in the initial findings, out of the seventy relevant hits, only eleven were related to incidents in the UK. The overwhelming majority were of abuse in the US (fifty-seven incidents) plus one in Ireland and one in Zambia. Thus, each of the most prevalent causes must be viewed with this US-centric standpoint in mind and according to Table 17 below.

Table 17: Twitter evidence – Abuse by cause

Abuse ⇨ / Cause ⇩	Non-secure disposal	Technical Security Failing	Loss	Theft	Unauthorised data: Disclosure or access	Unauthorised data: Retention
For self-gain (financial gain)				2 (TW15 TW40)	2 (TW47 TW60)	1 (TW34)
Third Parties		8 (TW5 TW6 TW10 TW16 TW22 TW41 TW69 TW70)		12 (TW4 TW7 TW9 TW33 TW35 TW44 TW45 TW49 TW58 TW66 TW67 TW68)		
Access without clinical or legitimate justification					6 (TW21 TW43 TW46 TW62 TW63 TW64)	
Facilitated by:						
Maladministration	8 (TW24 TW25 TW31 TW48 TW51 TW53 TW55 TW57)	7 (TW1 TW8 TW12 TW13 TW14 TW28 TW50)	6 (TW27 TW29 TW32 TW38 TW54 TW56)	6 (TW17 TW18 TW19 TW20 TW26 TW37)	3 (TW30 TW52 TW61)	
Human error			3 (TW2 TW11 TW59)		6 (TW3 TW23 TW36 TW39 TW42 TW65)	
Total by abuse type	**8 (11.5%)**	**15 (21%)**	**9 (13%)**	**20 (29%)**	**17 (24%)**	**1 (1.5%)**

7.B.3.B Theft

The most prevalent cause for abuse of health or biomedical data that emerged from the Twitter evidence was attributed to theft, totalling twenty incidents (or 29% of total incidents). Causes attributed to theft included those carried out by third parties (external to an organisation, with no explicit motive); for self-gain (where explicit self-gain motives were made): or because of maladministration (access to the data was facilitated by lack of encryption, password protection etc.). Of the twenty incidents of theft, eighteen occurred in the US, whilst only one occurred in the UK(TW45) and one in Zambia.(TW35)

Thefts carried out by third parties (external to the data controller as opposed to staff), represented twelve incidents (ten of which occurred in the US). In these cases, it is possible that the organisations and premises were specifically targeted by those with interests in selling data on the black market and/or were carried out by sophisticated criminals:

- In Zambia, the press reported the looting of computers that stored vital data for patients at the Cancer Diseases Hospital, which included data storage devices. (TW35)
- Regarding the only UK case of theft, a system used by the company *Pharmacyrepublic*, to record the medication handed out to around 2000 patients, was stolen from one of its premises. (TW45)
- In the US, fifty-seven hard drives were stolen from an insurance company's training facility. (TW68)

Insofar as the two incidents of theft with explicit evidence of being motivated by self-gain, both occurred in the US and involved former hospital employees selling patient data for profit. (TW15, TW40)

This is in contrast to the final category of thefts – those facilitated by maladministration – all of which occurred in the US (six incidents). These cases of theft were differentiated and collectively categorised as 'maladministration' because the thefts were made possible (or easier) due to poor technical security practices on the devices stolen or generally by the poor data handling practices of the data controller (potentially reflective of poor staff training). In five of the incidents, it was clear that the data were unencrypted, and thus when stolen, more easily accessible for abuse. (TW17, TW19, TW20, TW26, TW37)

A theme emerged in regards to thefts from employee cars – if the devices stolen were in plain view (even if in a locked car and regardless of data encryption) this could further incentivise theft (TW33, TW49) and be indicative of the need for further training with disincentives to handle data/devices carelessly by employees and independent contractors. A final theme worth noting is in regards to thefts while employees are travelling on vacation – these incidents could indicate the need to have clearer policies on the encryption of portable media (USB drives, laptops) and/or to prohibit the transfer or carrying of certain digital files to non-

work locations (i.e. acceptable for a business trip or home, but not so for annual leave and other personal time off)[TW37, TW26] or prohibit download of certain sensitive data to external devices at all.

7.B.3.C Unauthorised disclosure or access

The second most prevalent abuse type, unauthorised disclosure or access represented seventeen incidents (24%). The causes attributed to unauthorised disclosures or access related to incidents motivated by self-gain; incidents where access was given without clinical or otherwise legitimate justification; those due to more systemic, maladministration problems; and finally, inadvertent disclosures due to human error.

Taking each of these causes in turn, the most prevalent cause for unauthorised access or disclosure involved access without clinical or otherwise legitimate justification (6 incidents). These incidents all occurred in the US except for one in the UK, and always included access by employees who presumably had the technical security credentials to facilitate such access. These included situations where:

- In the single incident occurring in the UK (*not* reported in the UK hard evidence Section 7.A.1 above), a hospital employee accessed her ex-boyfriend's medical records without any legitimate or clinical reasons to do so.[TW46]
- Medical staff accessed patient records simply because they 'used to know the patient'.[TW62]
- Again, medical staff accessed patient records simply because they were 'curious'.[TW64]

Tied for the most prevalent *type* of unauthorised disclosure or access were those cases due to human error – which poses problems for its ability to be confused with maladministration. Similar to how 'borderline' incidents were assigned human error or maladministration in the hard evidence, incidents were considered due to human error if they were perceived as caused by the isolated mistake of a single individual, as opposed to being indicative of widespread administrative issues in data handling. Unlike other evidence, cases of human error featured a higher number of UK cases (four UK versus two in the US):

- In the UK, an Ayshire woman had her medical records mistakenly transferred from her GP (without her knowledge) to another practice in Manchester. Due to this mistake she was removed from screening programmes for cervical cancer years earlier, and found this out when she went in with symptoms consistent with cervical cancer).[TW42]
- In the UK, an NHS trust was fined following the exposure of three patients' medical data because faxes were sent to members of the public that included details on physical and mental health. (This was also reported in the hard evidence).[TW23, ICOM4]

- In the UK, a FOI request mistakenly revealed unrequested data regarding an operation, including sensitive personal data of individuals' medical issues.(TW36)
- In the US electronic, patient files with 'limited patient information' were sent to the wrong insurance company.(TW3)

Systemic problems in the governance over *legitimate and authorised* access (maladministration**)**, were the cause of three incidents of unauthorised access or disclosure, including two incidents in the US and one in Ireland:

- In the US, an employee gained unauthorised access to patients' personal information due to poor security standards.(TW30)
- In Ireland, a hospital outsourced transcription of medical records and GP letters to the Philippines. The identity of patients may have been disclosed (i.e. the records were not sufficiently anonymised and some records were never returned).(TW52, Ti9)
- In the US, a hospital employee allowed their friend into a restricted area where they could overhear patients' consultations describing their health condition.(TW61)

These instances reveal potential weaknesses in the organisations' training of staff on confidentiality of patient data at various stages of the patient care experience i.e. from the point at which the patient is admitted, to consultations with the doctors or nurses, to when records are filed and/or transcribed for future access and so forth. Providing accessible training on the different ways in which data could be improperly disclosed or accessed is important to prevent such abuse. We return to this point in Section 8.A.

Finally, the two incidents involving unauthorised access due to motivations of **self-gain** both occurred in the US by a medical employee. In the first case, the employee accessed patient data of a competing medical practice in order to send those patients marketing materials for his practice.(TW47) In the second incident, a radiologist accessed 177 pregnant mothers' patient records because she had lost a baby due to drug addiction and wanted to find out how similarly situated mothers received help to combat their drug addiction.(TW60) One can differentiate these two incidents on the basis of the pecuniary motivations in the former, and the emotional or non-pecuniary motivations in the latter.

7.B.3.D Technical security failures

Fifteen incidents were caused by technical security failures (21%). These could be attributed to either third party hackers preying on system vulnerabilities or to poor technical security not implemented properly (maladministration). It was expected that technical security failures would represent a large portion of the evidence – however this abuse type featured strongly only in the Twitter evidence as opposed to one incident reported in the hard.(ICOM1)

Technical security failed due to the intrusions by third parties – namely hackers – in eight incidents (all in the US). These included incidents of scale that could have been targeted for re-sale on the black market:

- A hacker accessed a medical providers' system, stealing the social security numbers and medical information of 9,700 clients. (TW6)
- A server containing the Medicaid (insurance) patient data of 280,000 Utah citizens was hacked and downloaded. (TW41)
- A computer server storing data for a state mammography registry was subject to a "targeted in a computer hack". Importantly, an individual whose data was breached was not aware that her mammography records were even sent to a registry in the first place (she did not know the registry even existed). (TW69)

The sheer scale of patient files that were accessed and exposed, presumably in spite of strong technical security measures, could indicate sophisticated criminality at work and the possible motivation to sell data on the black market.[150] Importantly, despite the lack of evidence of such hack-attacks in the UK, this does not (*in the slightest*) indicate that this has *not* occurred. As stated previously, there are mandatory data breach notification laws in the US, making such incidents come to light more readily than in the UK where the only organisations with mandates to report are within the NHS. This is something the ICO has advised to take account of when looking at trends of data breaches in the UK: where the NHS and public sector always have higher *reported* instances of data breaches – but not necessarily higher instances overall if private sector organisations are not reporting these incidents.[151]

Technical security failures could also be attributed to maladministration (seven incidents) – due to poor (or lack of) implementation of proper technical security and/or data handling protocol. In the seven incidents, organisations posted sensitive information about their staff or patients online, under the false assumption that it was *not* publicly available - when in fact, it was generally accessible; (TW1, TW8 TW50) held data on servers that were easily breached by hackers; (TW12, TW28) or found sensitive personal data regarding patients online unbeknownst to staff as to how the data were stolen.(TW13, TW14)

[150] Whereas the three evidence strands often consider abuses as they relate to *individuals*, others such as those related to hack-attacks, relate to the abuse of *many* (sometimes thousands) of people. Section 8 will consider individual versus large-scale impacts considering any meaningful distinctions between the scale of abuse that occurred. Further, we address cybercrime later in 9.D.1 The black market for data.

[151] This is not to undermine the severity or concern caused by the amount of data breaches that are occurring within the NHS. However, the presence of a mandatory reporting scheme, applicable only to a *portion* of data controllers in the UK, can and does skew the results on 'trends' of data breaches in the UK, as reported by the ICO. ICO, 'Trends' (2014) <http://ico.org.uk/enforcement/trends> accessed 26 April 2014.

7.B.3.E Other motivations for abuse

Table 24 in the Appendix reveals further incidents of abuse, including nine incidents where health or biomedical data were ***lost*** either due to maladministration(TW27, TW29, TW32, TW38, TW54, TW56) or human error.(TW2, TW11, TW59) Loss of digital or manual copies of data due to *maladministration* were considered to be indicative of more systemic, organisational problems as to the proper handling of data – these incidents seemed to be caused by maladministration at least more than equal to any element of human error. Whereas in cases of loss involving *human error*, the incident was considered to represent an isolated, one-off mistake, down to individual circumstance.

Eight incidents involved the non-secure disposal of health or biomedical data (see Table 24 in the Appendix). Non-secure disposal was to a lesser extent indicative of poor vetting of third-party vendors charged with the secure destruction of sensitive data(TW24) rather than a more blatant disregard for proper procedure – in seven out of the eight incidents, sensitive patient files were literally thrown away in publicly accessible bins or similar.(TW25, TW31, TW48, TW51, TW53, TW55, TW57) Despite the overwhelmingly US-centric nature of the Twitter evidence, the UK featured more in this category than did the US (four out of the seven incidents occurred in the UK). Finally, there was only one incident of unauthorised retention of data.(TW34)

7.B.3.F Categories of harm in the Twitter evidence

Similar to the other typologies created, a single incident could be interpreted from the Twitter evidence as causing more than one type of harm (indicated with an asterisk in Table 18 below). Thirty-six incidents, however, featured *no* discussion of harm at all – in such cases, the discussion of abuse of health or biomedical data was completely removed from any consideration of harm or potential harm caused to individuals, organisations or broader public interests. Therefore, in these cases it was not possible to infer even *potential* harm due to insufficient reporting of the incident, which does not necessarily mean no harm occurred.

Table 18: Twitter – Abuse by Harm

Abuse⇨ / Impact⇩	Non-secure disposal	Technical Security Failing	Loss	Theft	Unauthorised		
					Disclosure or access	Retention	Total by harm
Individual distress		3 (TW5* TW50* TW69)	1 (TW38*)	2 (TW9* TW35*)	3 (TW42 TW46* TW47)		**9**
Suboptimal clinical care				1 (TW35*)			**1**
Financial Loss		1 (TW5*)		1 (TW15)	1 (TW46*)		**3**
No discussion of individual harm	5 (TW25 TW31 TW53 TW55 TW57)	6 (TW1 TW13 TW14 TW16 TW22)	2 (TW2 TW29)	9 (TW18 TW19 TW20 TW37 TW44 TW45 TW49 TW66 TW67)	13 (TW3 TW23 TW30 TW36 TW39 TW40 TW43 TW52 TW60 TW61 TW62 TW63 TW64 TW65)	1 (TW34)	**36**
***No* harm**				1 (TW7)			**1**
***Potential* for harm**	2 (TW24 TW48)	8 (TW6 TW8 TW10 TW12 TW28 TW41 TW50* TW70)	7 (TW11 TW27 TW32 TW54 TW56 TW59 TW68)	7 (TW4 TW9* TW17 TW26 TW33 TW58 TW68)	1 (TW21)		**25**
Damage to institution	1 (TW51)		1 (TW38*)				**2**

*Indicate multiple types of harm for one incident

7.B.3.G Potential harm

Notwithstanding, in twenty-five incidents (35%), we *could* infer the *potential* for harm to occur in future, given the more substantial reporting in these incidents. First, as stated above, the majority of evidence identified from Twitter was from the US (fifty-seven of seventy incidents). In regards to the twenty-five incidents of potential harm, potential for *financial* harm was typically found when a US citizen's social security number was comprised thus enabling identity theft.(TW4, TW6) The potential for either financial harm or emotional/physical distress was found more generally in cases where data were left compromised and accessible to the public or left in the hands of hackers for an extended period of time.(TW1)

7.B.3.H Actual harm

In fewer cases, incidents of *actual* harm were uncovered – nine cases of individual distress ranging from distress caused by identity theft,(TW5) to general feelings of distress after being notified of their sensitive data being breached,(TW50) to incidents of harassment causing severe distress and impact on the individual's mental health.(TW46)

An exceptional case of both individual distress and the provision of hampering clinical care occurred in Zambia, whereby the theft of computers from a cancer hospital brought operations to a halt for the 350 patients. This caused severe individual distress and negatively affected patient care.(TW35)

Three incidents recorded the financial loss of individuals. This was typically in relation to identity theft;(TW5, TW15, TW46) whereby two incidents recorded damage to broader public interests, through the diminishment of public trust in the NHS.(TW38, TW51)

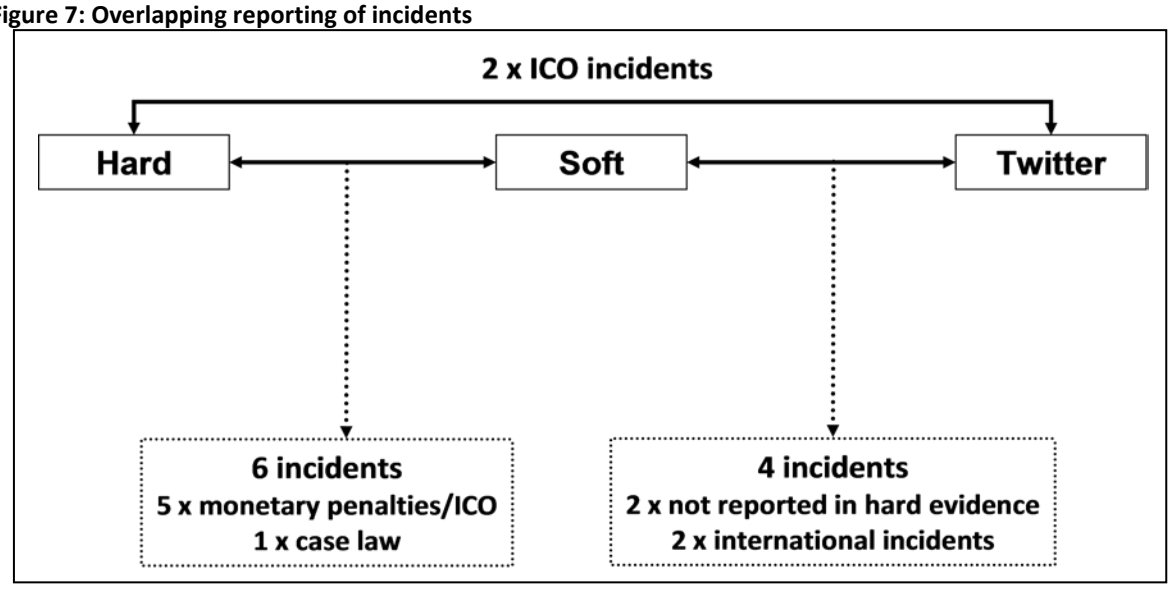
7.B.3.I No harm – but compensation

Important to note is the single case where a US Court recently found *no* harm but still awarded $3M USD in damages to the individuals whose data were exposed in a data breach. This ruling was based on the company's negligence, breach of contract, breach of fiduciary duty and unjust enrichment. Key to finding in favour of the individuals (despite finding no harm) was that the company purported, to its customers, that it would keep their data safe and clearly did not do so when laptops stolen from their staff exposed the patient records of tens of thousands of its customers.(TW7)

7.C Merged evidence

The merged evidence represents where the hard, soft and Twitter evidence strands produced overlapping results. A brief overview is shown in Figure 7 below and these incidents of overlap are highlighted in the Appendix.

Figure 7: Overlapping reporting of incidents



7.C.1 Overlap between hard and soft evidence

There were only six incidents reported in the hard evidence that were also reported in the soft evidence (via newspapers). Five such overlapping incidents were related to ICO monetary penalties, which are publicly reported on the ICO website and thus more easily transposed and noticed in traditional media outlets. It can be said that where the hard and soft evidence *merged*, that these cases represented the more egregious abuses in the hard evidence (though not necessarily so for the soft evidence). The single UK case law incident that overlapped with the soft evidence was regarding the highly publicised BBC news feature on falsification of hospital waiting times.[UKC9, Te9] Far more egregious cases involving the abuse of health or biomedical data, that were tried in either the UK or ECtHR or CJEU, were simply not picked up in the traditional media sources searched in the soft evidence strand.

7.C.2 Overlap between hard, soft and Twitter evidence

We further show in Figure 7 where the hard, soft (newspaper) and Twitter evidence overlapped (also highlighted in the Appendix). Only six incidents reported on Twitter overlapped with either the hard or soft newspapers searches.

Only two incidents reported in the *hard* evidence overlapped with those reported in Twitter. These two incidents similarly involved ICO monetary penalties and would be more easily picked up by social media outlets due to the ICO's publication scheme for issuing such penalties.

Only four incidents overlapped between Twitter and the soft (newspapers) search. These overlaps included two *international* incidents – one in Ireland[(TW52, Ti9)] and one in the US.[(TW1, Ma18)] The remaining two incidents related to abuses that were interestingly enough *not* reported in the hard evidence despite the likely involvement of the authorities and/or ICO due to the flagrancy of the abuses (i.e. the disposal of confidential medical records in a woman's garden in Londonderry;[(TW25, B4)] the disposal of eighteen patients' records in a communal waste bin at a residential apartment block and the disposal of a patient's sensitive medical procedures and test results in a bin outside Coventry University Hospital.[(TW48, G16)]

7.C.3 Useful comparisons between the evidence strands

Comparing the evidence types and their usefulness for a review such as this, the results from a hard evidence search could be described as 'what you seek is what you get'. In contrast, it would appear that Twitter lends itself well when considering the international, albeit US-centric, landscape. The lack of overlaps between the hard and soft evidence demonstrates that a newspaper search produces a broader picture of public interest and citizens' concerns. It is here that the voice of the public and advocacy groups can be heard (though heard only in a modest number of articles). Information gleaned in this fashion does come at a price. The reliability of a piece of evidence might not be unquestionable and the interpretation of such evidence relies on the academic judgement of the research team. Finally, in order to gather evidence from vulnerable groups, we suggest that web-based research is inadequate. Rather and quite rightly so, one should seek permission from those groups to access more forthcoming sources.

In summary, the clear lack of merged or overlapping results simultaneously indicates the limitations of the hard evidence versus soft evidence versus Twitter search on their own, whilst highlighting the value added by *combining* the three approaches. The three-strand approach offers a more complete and holistic view on the types of abuses and harms at stake when processing health and biomedical data.

8. Conclusions

8.A Conclusions drawn from the hard evidence

Given the narrow conception of harm provided for in law and even narrower provision for compensation, it was not surprising that the hard evidence uncovered a modest amount of evidence revealing *actual* harm.[152] However, the level of factual detail provided in court judgments and ICO enforcement procedures as to the type of abuse (i.e. reason for the claim), the cause (i.e. to establish fault, negligence etc.) and in considering the award of damages (i.e. for any pecuniary or non-pecuniary harm caused) contributes greatly to a clearer understanding of the types of circumstances that lead to abuse of health or biomedical data. The hard evidence thus provides rigorous detail as to abuse type and causes in a way that sources in the news or social media cannot provide (with the same degree of certainty).

As to the most prevalent abuse types and causes of abuse (maladministration; using data against the objections or without the consent of individuals; human error; or unauthorised disclosures by the press or media) – conclusions drawn feature strong implications for governance and thus warrant separate discussion in Section 9.A below.

8.A.1 Evidence of individual impact lacking

What *was* genuinely lacking from the hard evidence was any sense of the voice of the individuals implicated – the court or ICO discussed harm far removed from the (likely) broader, *perceived* harm experienced by the affected individuals and typically only *inferred* harm that could arise. This was evidenced in the overwhelming 53% of cases where only a *potential* for harm was found (as opposed to actual harm). Evidence of actual harm featured less frequently. Where actual harm was found, it was in cases where the circumstances dealt with particularly sensitive data (such as HIV-positive status, rape, abortion) or where criminal offences were being tried (as opposed to 'ordinary' contraventions of the DPA which come under civil law jurisdiction). Thus what the individuals may have subjectively *perceived* as harmful would simply have been left out if not relevant to the particulars of the claim in front of the adjudicating body.

8.A.2 Understanding risks for harm – actual versus potential harm

The hard evidence uncovered individual distress (either purely emotional or with physical manifestations) as the most prevalent form of *actual* harm associated with abuses of health or biomedical data. Importantly, individual distress *is* provided for under the DPA – individuals

[152] See Section 3.B above for fuller discussion on the narrow conception of harm under the law.

can recover for individual distress – albeit in limited circumstances.[153] In light of the fact that the law specifically takes into account (arguably insufficiently) individual distress when calculating damages, it makes sense that this form of *actual* harm was well represented.

Financial loss (damages) is also specifically accounted for in the compensation provided under the DPA section 13 but only featured in four incidents. Thus, it would seem that individual distress, whether purely emotional and/or physical *is* the most prevalent risk that data controllers should consider when processing health and biomedical data. This is with the specific understanding that *these* harms *are* specifically recognised by the law (and thus can be compensated for).

However, the *potential* for harm was taken into account by the ICO when issuing monetary penalties for serious breaches of the DPA. Where the prospect for harm remained a grave possibility for the individuals implicated by a particular data breach, the ICO took this into specific account when issuing the penalty. Thus data controllers might consider the risks for harm on a spectrum of harms most likely to least likely to occur, with the understanding that if a strong potential for harm is found due to the nature of breach (e.g. if lost or stolen hardware is never recovered or the data is so sensitive that the risk for future abuse is high) this can be enough to support a hefty monetary fine – actual harm is *not* a necessary element to the ICO imposing fines for breaches of the DPA. The level of fines exacted on organisations that have not taken appropriate measures to eliminate risks or reduce possible impact to individuals, is warranted where such risks have not been taken into account or blatantly disregarded when warned previously by the ICO.

8.A.3 Harms to the public interest

As stated before, harms to the public interest are simply not provided for in the same way as individual damages are under the DPA, due in large part to the remit of the DPA that is over *personal* data. Thus, instances of harm caused to the reputation of public organisations such as the NHS or to broader public interests, such as in the diminished confidence in the doctor-patient relationship are not provided for. Furthermore, outwith Freedom of Information Act requirements, there are no positive obligations to *use* data and as such, harms caused by failure to use data are similarly not recognised in law. Notwithstanding, the courts *did* consider the harm that certain uses (abuses) of health or biomedical data had on broader public interests regarding the confidentiality of the doctor-patient relationship and the disincentives that this could cause persons to *not* seek the treatment they need.(IT1, EUC1) They also considered harm caused to other confidential relationships(UKC5, ICOD4) (e.g. interactions with Human Resources), as well as the damage to the reputation of a public service such as the NHS.(UKC9)

[153] DPA s 13(a), (b) provide that an individual may only recover for individual distress arising out of contravention of the DPA *if* (a) the distress also causes the individual to suffer damages (financial); *or* if (b) the distress arises out of use of the data for the "special purposes" (i.e. journalism, arts, literature).

From this evidence, it would appear that courts *will* take into account harm to broader public interests (such as the confidentiality of certain relationships) and will do much to uphold the necessary, confidential quality of these interactions. Whilst damage to the reputation of a public service might also be taken into account, it is considered that this would always take a backseat to evidence of *individual* harm, with greater emphasis being put on the presence of the latter, which was clearly featured more in the hard evidence section. This is even more apparent in the soft evidence, which will be concluded upon below.

8.A.4 Harms outwith privacy harms

One of the central conclusions of this report is the need for a holistic approach to conceptualising harm in context of processing health and biomedical data outwith the narrow scope provided for in law. The implications arising out of the single, legal case where the court unequivocally found *no* harm,(UKC14) because the data were anonymised, raises important questions regarding the range of interests that are impacted when individuals' health and biomedical data are used.

In *R v Department of Health, ex parte Source Informatics Ltd*[154] the High Court's determination that *no* harm occurred hinged upon the prescription data of patients being *anonymised*. The High Court's reasoning was that if anonymised data were used – even if for a commercial purpose and without the prior notice of this to the patients – no harm could be caused. Thus, '[i]n the Court's view, concealment of the confider's personal identity in any further disclosures of the confided information is sufficient to secure the protection of the confider's personal privacy.'[155] The approach taken by the High Court raises questions about the use of data for research and where they are (a) suitably anonymised and (b) used without consent but authorised by a body such as the Confidentiality Advisory Group in England under s 251 of the 2006 Act, or the equivalent in Scotland through the working of the Privacy Advisory Committee.

If we accept that the law 'recognises much more than a right to concealment of one's identity as falling under a right to privacy'[156] then the High Court's judgment fails to account for a host of other human interests which are at stake in the processing of health and biomedical data – namely autonomy, identity and dignity.[157] The implications of this for good governance are such that anonymisation *alone* may not be sufficient to recognise the full range of interests at stake when processing biomedical and health data. Whilst anonymisation of data technically brings use outwith the remit of the DPA, *good* governance would require transparent

[154] [2001] QB 424, [2000] 1 All ER 786.
[155] Beyleveld and Histed, 'Betrayal of confidence in the Court of Appeal' 280.
[156] Beyleveld and Histed, 'Betrayal of confidence in the Court of Appeal' 295.
[157] However it is understood and exemplified by the evidence produced in this review that '[w]hile the existence of affront might be real, it is not obvious what the legitimate legal interest is that would be compromised'. See: Laurie and Harmon, 'Through the Thicket and Across the Divide' 9.

consideration of the full range of human interests at stake.[158] Thus it is contended that anonymisation is not in and of itself enough, in recognition of the vast spectrum of material harms and soft impacts that can arise out of processing health and biomedical data.

8.B Soft evidence

This strand of the research sought to identify evidence of actual harm to the individual or to social groups through the abuse of biomedical or health data. We argued that it is the individual subject of an abuse who is best placed decide whether a harm has affected him or her and to what degree, because the effect of the harm can only be subjective. We also explained why we found the term 'harm' inappropriate in this context: the *impact* of the harm is at the forefront.

We presented one hundred and thirty-nine scrutinised articles that were collapsed into sixty separate incidents (Section 7.A.2 *Soft Evidence*). Some incidents may have had multiple impacts (Section 7.B.2 *Soft evidence typology*). Therefore, the number of incidents and impacts do not tally.

8.B.1 Abuse in the biomedical and healthcare sectors

The majority of abuses involved NHS staff, or in the case of theft, NHS premises including GP surgeries/care homes (total incidents = 48). In contrast, only a quarter of incidents were outside of the NHS (total incidents = 11). We found no evidence of abuse in academic institutions in the UK that hold biomedical and health data. The high incident rate would appear to be in line with official ICO figures regarding data breach figures across all sectors in the UK.[159]

Taken at face value, this might be taken to suggest that this sector is weaker in its security and governance than others. However, the NHS holds a huge amount of data and data transactions are immense. The high rate of abuse may, therefore, reflect a rate by volume effect. It should further be taken into account that

(a) in contrast to other sectors, the NHS is obliged to report breaches.

(b) The NHS is high in public interest, so breaches and other failings are reported widely in the press.

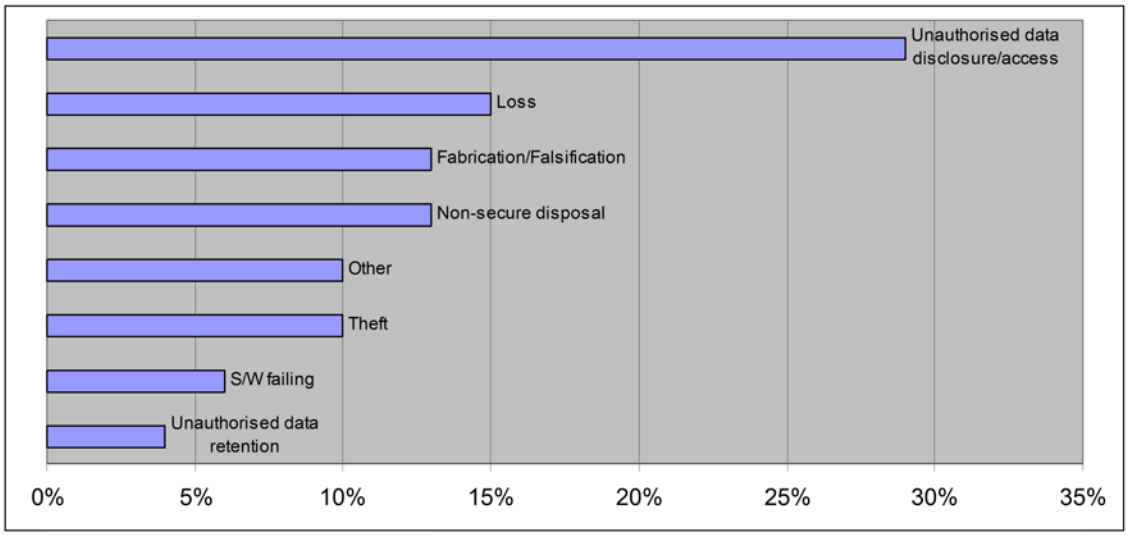
[158] The ICO in its 'Anonymisation Code of Practice' discusses the need for transparency – whilst it might not be feasibly possible to notify all individuals of intended anonymisation of their data, governance policies should indicate how personal data will be used, including whether anonymisation will be performed. ICO, 'Anonymisation Code of Practice' 40.
[159] ICO, 'Enforcement: Trends' <http://ico.org.uk/enforcement/trends> accessed 20 June 2014.

(c) The rise in accident/injury claims lawyers advertising for business and the resulting claim culture might have a role in 'chasing for cases' of breaches more so from the NHS than in other sectors.

8.B.2 Types of abuse

In Table 14 it was noted that 48 incidents involved NHS staff, and 11 incidents non-NHS staff. The majority of incidents involving non-NHS staff arose in the main because the abusers were at the receiving end of intentional and unintentional actions by NHS staff. We conclude therefore on the findings involving NHS staff only. The majority of abuses (29%) were due to unauthorised data disclosure or access. However, loss and theft together accounted for a further 25%, non-secure disposal for 13% and fabrication/falsification a further 13%. As shown in Figure 8 below, we see, therefore, a spread of abuse types.

Figure 8: Soft evidence – Types of abuse

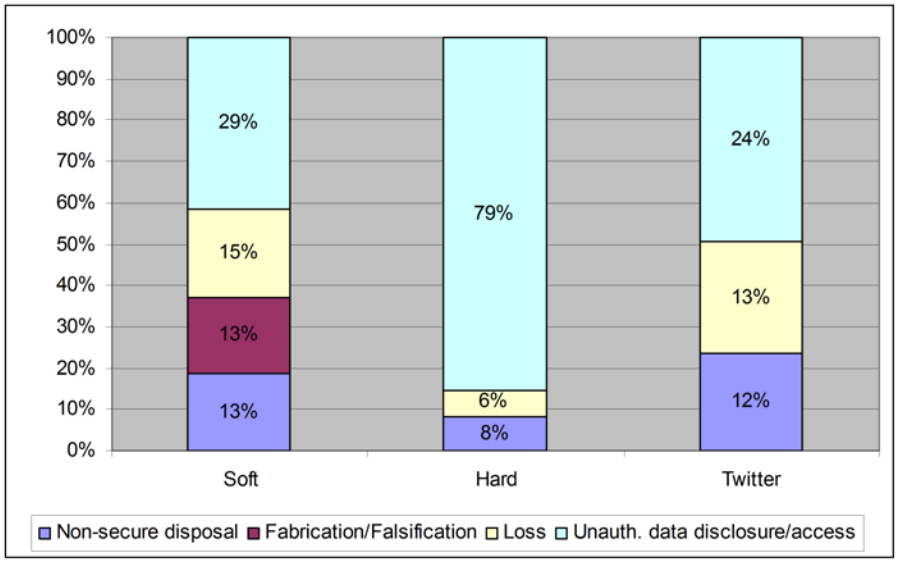


We compare the four most frequent types of abuse identified in this strand to the rates identified in the other two strands (see Figure 9 below) and can conclude the following. The hard evidence strand clearly was the best source to identify cases of unauthorised data disclosure/access, where such abuse was identified in just under a third of the cases (29%) in the soft evidence. Non-secure disposal cases were picked up approximately equally in the three strands (8-13%). Interestingly, abuse due to data loss accounted for only 6% of incidents in the hard evidence, yet 15% and 13% in the soft evidence and Twitter evidence respectively.

Most importantly, only the soft evidence was able to provide evidence of fabrication/falsification (except for the exception of one case in the hard evidence[160]). Including such instances may be a novel approach to some, and it does have the flavour of deliberate loss and/or destruction of paper records. This has far-reaching consequences in determining the sources to consult when calculating data abuse prevalence rates.

[160] *Henry v British Broadcasting Corporation* [2005] All ER (D) 43. (Incident number UKC9)

Figure 9: Comparing types of abuse across the three evidence strands



8.B.3 Causes of abuse – the motivations to abuse

In only seven incidents was it possible to identify clearly the motivation behind the abuse. Three of these were linked to management failings and scandals, and all resulted from the perceived need to meet targets now commonplace in the NHS culture (see Table 14). The other five involved individuals acting inappropriately to protect their professional reputations after severe failings in the care given or for personal gain. Comparing these figures to the hard and the Twitter evidence, only two incidents in the hard evidence were to meet NHS targets, and four in Twitter for personal gain.

These seven incidents may well be just the tip of an iceberg, because internal NHS investigations are often subject to confidentiality, and it may require a FoI request for findings to come to light. Additionally, even the Health Service Ombudsman is in 2014 facing allegations that it disregards the majority of complaints it receives. It conducts investigations in private and does not discuss individual complaints.[(Te08)] Thus, the use of confidentiality clauses, we conclude, reinforces the suspected tip of the iceberg.

8.B.4 Facilitation of abuse – maladministration and human error

As stated earlier, we attempted to identify the factors that might facilitate the abuse. Due to the limitations imposed by interpreting the incidents from the soft evidence, there was a strong weighting towards maladministration, and little definitive evidence of human error. Therefore any conclusions must be considered with extreme caution.

According to our very broad categorisation (see Table 14), 45 incidents were due to maladministration, 7 to human error and 2 to misinterpretation of legal obligations. The incidents categorised as either maladministration or human error should be of particular interest, because they would help identify poor practice, and from that point it would be possible to work on solutions. It goes beyond the remit of this report to investigate further the

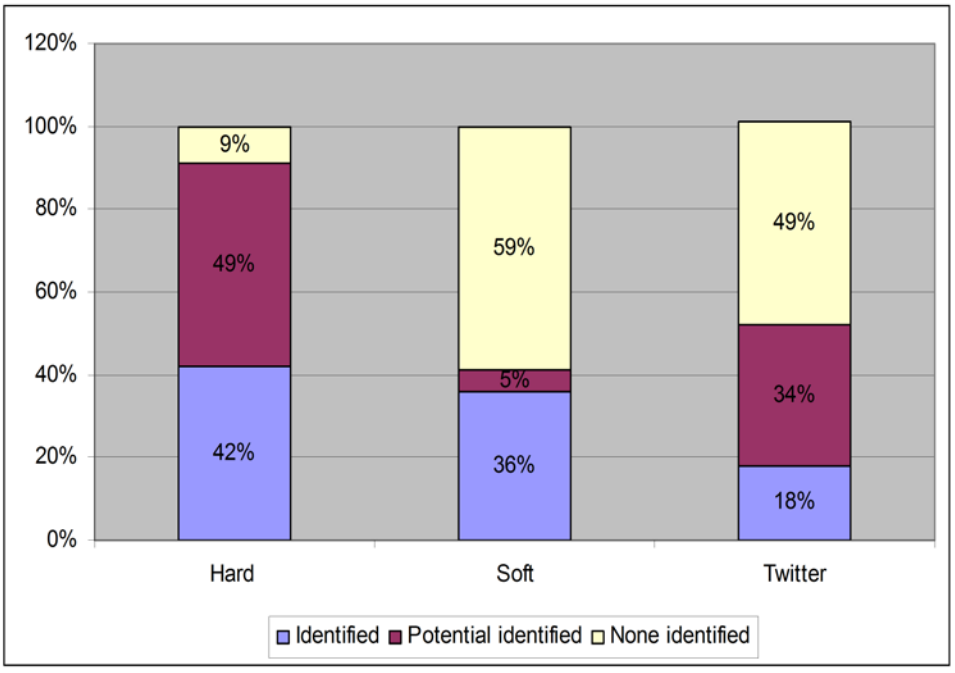
why and how that such incidents occurred. Rather than speculating here, we give clear recommendations under Section 10 *Future Research*.

8.B.5 Impacts of abuse

It is useful to consider these findings in the comparative setting (see Section 7.C *Merged evidence*), because one aspect of this work was to look for evidence of impact in the grey literature. By comparing the three strands, we can gauge how forthcoming the grey literature was.

Impact identified: The rate for identifying impact was lower in the newspaper strand (36%) than in the hard evidence (42%), but more frequently than in the Twitter evidence (18%). One would have expected newspaper articles to report impact more frequently, given that journalists are able to bring in personal interest aspects to their articles (in some newspaper types more than others). Nonetheless, the soft evidence strand did offer often very moving impact statements from the subjects or the loved ones of data abuse, and we consider this to be one of the key strengths of the soft search results.

Figure 10:Comparing frequencies of impact/harm across the three evidence strands



Potential for harm/impact identified: Only 5% of soft incidents reported the potential for impact. This is unusual, when we consider that cases of data breach in the NHS, where thousands or indeed millions of patients might be affected by an abuse. However, perhaps the breach itself is newsworthy enough. Examples of this can be seen in the following headlines; '*NHS trust fined record £325,000 for auctioning off online computer hard drives filled with HIV patients' details*'(Ma12) and '*Records stolen from hospital that held secret DNA database.*'(Ti13) On the other hand, how could a journalist then track down any individuals affected by a breach of hundreds to millions of patient data? The newspaper articles did sometimes include

statements from citizens' voice groups, and these were particularly forthcoming in addressing the potential for harm having an impact.

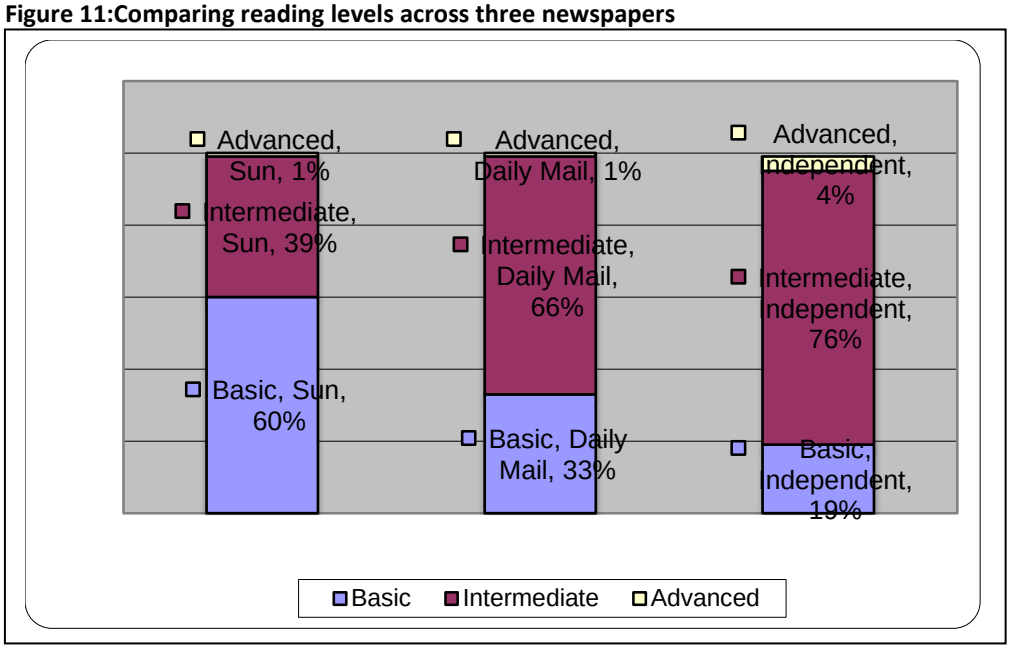
No impact identified: Fifty-nine per cent of newspaper articles did not discuss any impact. We reiterate here that this does not mean that no harm occurred in these incidents.

Finally, when comparing hard with soft evidence it becomes clear that it is part of a judge's ruling to identify a potential for harm or ascertain whether harm has occurred in the legal sense. It is therefore unsurprising that the soft evidence produced fewer instances of harm/impact or harm/impact potential than the hard evidence did, and thus a high rate of incidents where no harm was addressed (59%). The rates from the soft evidence raise two questions. Is there more harm/impact than acknowledged in the public domain? If so, how can this be quantified?

8.B.6 Quality of findings in newspapers

There were differences in the way that specific newspaper types reported the incidents. A newspaper writes for its readership, and as we presented in Table 6, these can range from tabloid to broadsheet, from right-wing to centre-left. These differences can account for the level of language used, the balance between information and opinion and, not least, how the newspaper 'feeds' its message to the reader.[161] It would appear that each newspaper has a majority audience of one language level or another (see Figure 11:Comparing reading levels across three newspapers) and from this it is clear that some articles/incidents can be reported in a more sophisticated way than others.[162]

Figure 11:Comparing reading levels across three newspapers



[161] There is the debate as to whether the media influence their audiences or merely give their audiences what they want. It is possible that these are symbiotic relationships.
[162] 'Google's reading age tool - comparing UK newspapers' (*Virtualeconomics.co.uk*, 2010) <http://www.virtualeconomics.co.uk/2010/12/googles-reading-age-tool-comparing-uk-newspapers.html> accessed 20 June 2014.

Against this complex backdrop, we ascertained that often very little information could be found in tabloid articles.[163] Although such articles served well to gauge the mood of its readership, it is questionable just how useful tabloid articles are for the purposes of research such as this. Articles from middle-market newspapers gave enough information overall to consider the article for relevance, more so for the Daily Mail.[164] As seen above, 66% of the Mail's readership have an intermediate reading age, and this goes some way to account for the amount of useable information contained in articles. (Former) broadsheets were very well informed written in a sophisticated language, and their articles would provide a good starting point for further research.

On a final note, it was an interesting exercise to read and compare the use of emotive and/or suggestive language used by different newspapers. It goes beyond the remit of this report to perform any discourse analysis, but here we give brief examples of what messages are transmitted and how, and which further implications/undertones can be found. The texts for each newspaper are direct quotations. In the first example (see Table 19: Discourse analysis – Telegraph and Guardian) the audiences targeted are centre-right (Telegraph) or centre-left (Guardian). Neither makes it clear that HES data extracts were supplied, both question the correctness of this and both link this to the care.data debate.

Table 19: Discourse analysis – Telegraph and Guardian

Incident: News53: Health records sold to Staple Inn Actuarial Society		
	The Telegraph (Te04)	**The Guardian** (G02)
1. Source	The Telegraph disclosed	It has emerged that ... according to the Daily Telegraph
2. What was done?	Hospital data covering 47 million patients was sold by the NHS for insurance purposes	A major insurance body bought more than a decade's worth of hospital data covering 47 million patients
3. Justification, mitigation	[HSCIC] would like to restate that full postcodes and dates of birth were not supplied	[HSCIC] insisted that the records were not used to analyse individual insurance premiums
4. However, the reader should also know that ...	Predecessor body was wrong to sell the information	The details were then reportedly combined with information from credit ratings agencies
5. Linking to care.data	Those in charge of the new [care.data] scheme have repeatedly insisted that data held in the new giant database would never be used for insurance purposes.	The news comes at a time of heightened sensitivity ... The [care.data] project ... has been put on hold for six months.

[163] The Mirror and Sun.
[164] The Express, Mail, and Western Mail.

In the second example (see Table 20) the audiences targeted are right-wing (Daily Mail) or centre-left (Independent), with 66% and 76% resp. of its readership having an intermediate reading level. There are similarities between the texts, but also crucial differences. The first quotation from the Mail (Personal data ... was ... sold on auction site) is in the form of sub-headings, that is, the 'take-home message'. It is also misleading in that it could suggest intent. Both articles describe the patient groups affected, but only the Independent also reports on those NHS staff who are also subjects of the abuse, that is, victims are also close to home, not only patients. Finally the Mail notes the record fine of £325,000, but the Independent also presents the standpoint of the Trust, where the CEO not only raises the issue of austerity, but also translates what £325,000 can buy in patient care delivery.

Table 20: Discourse analysis – Telegraph and Independent

Incident: News18: NHS trust fined because hard drives containing patient information sold at auction		
	Daily Mail (Ma12)	**Independent** (In26)
1. What was done?	Personal data ... was ... sold on auction site. NHS Trust ... sold computer hard drives ....without first removing confidential details about patients with HIV.	Highly sensitive files of tens of thousands of patients, including details of HIV treatment, ended up being sold on eBay.
2. Other data subjects?	... included details of patients' medical conditions and treatment, disability living allowance forms and children's reports	Same as Mail, but also: ... documents containing staff details like National Insurance numbers, home addresses ... and information referring to criminal convictions and suspected offences
3. How discovered?	University contacted the [ICO] ... to advise that one of their students had purchased hard drives via an Internet auction site.	
4. The size of the fine and its impact	Record £325,000	In a time of austerity ... we simply cannot afford to pay a £325,000 fine. ... [The amount would pay for] the delivery of 300 babies, 50 hip operations, 30 heart bypasses and 360 chemotherapy treatments.

8.B.7 Quality of findings in charities and citizens' voice groups

There was a paucity of incidents identified through charities and citizens' voice groups. As we concluded earlier, charities support individuals with a set of concerns unique to that charity. Thus we found no evidence of harm or the impact of harm upon anyone because of their minority group membership.

We were particularly interested in the Terrence Higgins Trust website, not least because those living with HIV are not bound by age, ethnicity, socio-demographic status and so on. A substantial part of the site is for members only, all of whom live with HIV. With ethical approval (Swansea University's *College of Human and Health and College of Medicine Ethics Committee*) in place, we contacted the THT media team and found that they would be most helpful in gatekeeping/passing on information to their members in the framework of a larger future study. This is an interesting point to note, particularly because we found no evidence of discrimination or stigmatisation of lower-power/lower-status groups. The lack of evidence does not mean that there is no discrimination or stigmatisation.

In conclusion to the findings from charities and citizens' voice groups, there is clearly more work to be done to find out more. We make suggestions in Section 10 *Future Research*.

8.C Conclusions drawn from Twitter evidence

The incidents reported on Twitter were done so with varying levels of detail as to abuse type, cause and instances of harm. As such, the conclusions offered in this section relate to those instances of abuse and harm which offer the most detail given the medium of reporting. Since Twitter offers less concrete and rigorous evidence than the hard evidence, and given the US centric focus of the results, the incidents reported offer more insight into general trends of data breaches, whereas the UK results (in both the soft and hard evidence) offer more insight for UK governance of health or biomedical data. However and importantly, Twitter featured several incidents involving larger-scale data breaches, which may have implications beyond those, effectuated from smaller-scale data breaches impacting one or two individuals. The data breaches implicating 165,000(TW9) to 729,000(TW17) to 780,000(TW41) individuals arguably have greater *potential* for negative impact and harm on broader public interests. Abuses of health or biomedical data of such scale will likely engender more widespread and stronger feelings of mistrust regarding the organisations involved and in the confidentiality of the services implicated. Whilst there may be no differential in *actual* *individualised* harm there arguably is such a differential in terms of actual (or at least potential) harm to broader public interests.[165] Due to the unquantifiable nature of harms to broader public interests, it is impossible to speculate further as to any relevant threshold whereby the differential for increasing harm to broader public interest occurs. However, episodes implicating hundreds of thousands has relevance for determining measures of good governance in handling and maintaining large amounts of personal data.

8.C.1 Prevalent abuse types

Thefts, unauthorised disclosure or access, technical security failures and non-secure disposal of health or biomedical data featured heavily in the Twitter evidence.

[165] However, in particularly egregious abuses of health and biomedical data involving one or only a few individuals, if well publicized, can have a similarly great effect on broader public interests.

From the evidence, ***theft*** did not appear to be an issue featuring prominently in the UK (with only one incident out of twenty occurring in the UK, eighteen in the US, one in Zambia). This imbalance in incidents of theft could indicate a more highly developed black market for health data in the US as opposed to the UK;[166] and/or the increased effectiveness of criminal monitoring and/or data breach notifications in the US, where in the UK such notifications are not mandatory.

The second most prevalent abuse type **involved unauthorised disclosure or access of data** – whereby, access to the data in question without legitimate reason to do so, featured as prominently as with cases involving human error. We distinguished between the unauthorised access of data for reasons involving financial or otherwise personal self-gain, and access simply without proper reasons for doing so. The latter cases featured more prominently, a possible indication that more robust audit trails and access controls are needed when it comes to particularly sensitive data. In these cases, data was for the most part accessed for non-malicious reasons – to satisfy curiosity, possibly boredom or similar.

However, curiosity *can* still lead to harm if new (and especially sensitive medical) information is learned about a patient/individual that was not known before, and could be used against them in a discriminatory fashion.(EUC9) Thus, even when more malevolent motivations are lacking, data controllers should restrict access and thus ensure sufficient safeguards are in place that are commensurate with obligations of confidentiality and/or data protection to the individual involved.

Human error also played a significant role in the evidence of unauthorised disclosure or access. It emerged during the review that cases caused by human error could be rectified by different approaches to the administration of data, involving different staff training and/or entirely different data handling protocol. Importantly, the key elements involved in cases of human error –the human element and chance - cannot be removed. Thus, abuses caused by human error cannot be ruled out entirely - not even the best governance can prevent these instances of 'chance' or mistake entirely.

Technical security failures featured less prominently in the results than anticipated – if considering a 'traditional' or narrow conception of how a data breach involving health or biomedical data might occur. However, the even balance between *causes* for technical security failures (eight incidents caused by the technical prowess of a motivated intruder/hacker i.e. involving third parties; and seven caused by poor administration of technical security standards i.e. maladministration) has important implications for data controllers. First, that vigilance and adaptability to constantly changing technology is key to eliminating risks involved when storing sensitive health and biomedical data. Second, that data controllers must factor into their risk assessments 'motivated intruders' – they should assume

[166] The black market is discussed more generally in Section 9 below.

that '…there will be someone who would want to identify the individuals to whom it relates and who will use all methods reasonably available to do so.'[167]

The incidents involving technical security failures also highlight the permanency of digital footprints – even if a file is deleted, there are technologies such as caching, and that will leave a footprint. This makes it increasingly important to constantly review internal security measures against current, technical best practices. Organisations simply cannot underestimate the motivations or technical prowess of hackers – in two cases, the organisations did not even know their patient databases were hacked until it was too late and the files were exposed (or worse) shared on the black market online.

The ***loss*** of data was more indicative of wider systemic issues regarding organisations' data handling practices (maladministration), instead of human error. Maladministration was considered the *cause* of a particular abuse when not only a hard drive, USB stick or laptop was lost, but when that particular device was not encrypted or otherwise protected – thus *facilitating* easier access and abuse of the sensitive data.(TW27, TW29, TW32) These cases highlighted, once again, the importance of good technical security standards, implemented *across* an organisation. For instance, if a device cannot be recovered after a staff member loses it, but it can be wiped remotely; and furthermore, technical security measures can prevent certain, sensitive data from being downloaded at all onto portable devices. Such measures can diminish the chances of sensitive data being accessed and abused.

Finally, despite the US-centric nature of the Twitter evidence, the ***non-secure disposal of data*** seemed to be a particular problem in the UK where there was clear disregard for patient confidentiality and no sense of proper data protocols being understood or implemented by staff. When hospital staff are reverting to throwing confidential, patient files, (containing extremely sensitive health data) into public bins(TW48, TW53, TW57) or in similarly inappropriate and publicly accessible places(TW25, TW51, TW55), it is clear that (1) proper data handling procedures were not taught or thus understood sufficiently by staff; and or (2) the particular working environment breeds contempt and disregard for standard protocols and procedures in place.

8.C.1.A Misconceptions on level of harm uncovered

Fewer cases of actual harm were uncovered than anticipated in the Twitter evidence. Due to the less confining parameters (that governed the hard evidence search), it was expected that Twitter would uncover more incidents reported from the standpoint of the individual then it did. In fact the harm (or lack thereof) uncovered in the Twitter evidence, largely mirrors the reporting in the hard evidence – incidents featuring *no* discussion of harm and *potential* for harm featured most prominently. Also similar to the hard evidence strand was the most prevalent finding of *actual* harm being individual distress.

[167] The ICO, 'Anonymisation Code of Practice' 18.

In this regard, it is considered that the Twitter evidence sits squarely neither as hard evidence *nor* soft evidence. The incidents reported on Twitter would often link to secondary news reports focused on the factual circumstances of a particular abuse, leaving out the potentially more 'sensational' impact statements of the individuals involved. Just as in the hard evidence, harm was discussed entirely 'removed' from the individual perspective and thus did not provide the same type of insight gained from the newspaper search in the soft evidence strand. This lack of evidence of harm may be due to the very nature of Twitter, which relies heavily on links users make to external news sites in order to "create" news on *its* site.

The value added by undertaking this non-traditional approach to evidence gathering is understood now, as in part, to reveal the overall *lack* of time and discussion spent on the *objective* and *actual* individual and public *costs* associated with abuses of health or biomedical data. Even if in thirty-six out of seventy incidents reported on Twitter, no discussion of harm was provided – this simply does not indicate harm to individuals or the public interest did not occur. The importance of data controllers understanding, from a relatively objective basis, what actual and potential harms are at risk of happening when processing sensitive health and biomedical data, is key to ensuring proportionate and effective governance that seeks to prevent most instances of abuse found in this review.

9. Implications of the Evidence

This section looks at our conclusions, that is, the implications of our findings brought together with information reported in the Introduction. We present here and in this order the implications for governance, provide our assessment of the effectiveness of sanction, and conclude with a discussion of incentives and disincentives. Note that public engagement is a theme that is brought in across several of these sub-sections.

To address the secondary aim of this report – to find evidence of harm arising from non-use of data – we consider below the implications of non-use from the perspective of this review, and thus the lack of evidence found. Therefore, this section will feature a focused discussion on the lack of evidence found of harm arising from non-use of data. This discussion will offer insight into why evidence of harm from non-use is difficult to find. Importantly, this discussion will conclude with the implications of non-use for governance of health and biomedical data. Other implications of non-use are discussed elsewhere in this report (see Figure 14).

Our overall conclusion is:

The evidence identified shows a narrow range of sanctions available when health or biomedical data have been abused. It is considered that the sanctions applicable to the abuse of health or biomedical data in the UK are not entirely ineffective, but also not fully capable of offering robust disincentives for further abuse. Because the 'softer' or more pre-emptory sanctions imposed at the earlier stage of the complaints process are not publicised, it was not possible to assess the effectiveness of a potentially wide portion of 'sanctions' available. However, the effectiveness of sanctions imposed at later stages (usually post-abuse) are limited in the UK to the narrow confines of the DPA (for the ICO), and slightly less so for UK Courts that may take a broader perspective in line with common law and human rights. In this regard, the ECtHR serves an extremely important role as an alternative forum to address abuses that could be overlooked within any domestic system. However, all that the ECtHR can do is declare a breach of human rights; it always then falls back to the domestic offending state to change its laws and practices. In the next section, we consider the effectiveness of the remedies offered by these various sanctioning bodies – the ICO, Information Tribunal, UK Courts and ECtHR.

9.A Implications for governance

Due to the rigour necessary in justifying court and tribunal judgments as well as in ICO enforcement measures, the hard evidence provided more precise detail (than the soft evidence strand) as to 'what went wrong' in particular situations where use of health or biomedical data was considered an abuse. (On the other hand, there were only six single

incidents reported in the hard and soft evidence, so direct incident comparisons were limited.) As such, the hard evidence in particular will be drawn from to consider the implications for the governance of health or biomedical data in the UK.

However, the value added from approaching the evidence from a 'soft' perspective also reveals important implications for governance, because it relates to which harms and impact are taken into account and brought into the public eye. The soft evidence has revealed that a harm can result in an impact, and arguably governance should be as pre-emptive as possible (typically via ethics approval processes).

Thus, we advocate an approach to governance in light of both hard and soft conceptions of harm, by not only protecting against hard (actual) harm, but also being sensitive to potential impacts. These ill effects can be softened through good preparation and an understanding of likely expectations. We can never eliminate harm or impact entirely, but we can better prepare for both. Incidence of actual harm might seem the most severe, but impact is nonetheless significant and should be accounted for in good governance.

In this vein, we consider the most prevalent causes of abuse and the implications for governance. Given the focus of the report on finding evidence of actual harm, governance will be considered specifically from the vantage point of the evidence reviewed. In consideration of the most prevalent causes for abuse and the implications this has for governance, we address the relative effectiveness of the sanctions and remedies perceived in the evidence, in light of the prevalence of harm.

9.A.1 Maladministration (most prevalent cause for abuse)

The most prevalent cause for abuse across both hard and soft evidence was **maladministration**. Maladministration offers the most implications for governance as it is considered the epitome of *poor* governance. It was accepted that incidents involving alleged maladministration would be hard to 'call'. For example if patient records were stored in a public area before being taken to a safe storage area,(Inc39-E18) was this human error or maladministration or both? Similarly, if an unencrypted portable media drive was lost, how much of the data breach and any resultant harm is due to human error and/or due to the poor implementation of policies on proper technical security and data handling?(ICOM2)

In borderline cases and where incidents were perceived as *more* indicative of systemic organisational problems as to the proper handling of data, rather than human error, maladministration was considered the cause. Maladministration poses greater implications (and value) for understanding the causes of harm. Whereas the human factor (chance, mistake, etc.) can never be eliminated entirely, poor implementation of data handling procedures (here poor governance) can be improved and made fit for purpose, that is, made more robust to prevent instances of harm from occurring.

Due to the broad categorisation processes described above, maladministration operated as a catchall cause referring to incidents including those arising from:

- Failure to take any action when necessary to prevent an abuse;
- Failure to follow correct procedures or the law despite the provision of guidance and existence of standard procedures and protocols;
- Inadequate consultation prior to taking action;
- Lack of clear mandates on proper standard procedures and protocol; or
- The adherence to out-dated standards and procedures that put data at risk.

The maladministration of health and biomedical data most often resulted in the unauthorised disclosure of or access to health or biomedical data. The multiple level failings of the proper administration and handling of data, as it relates to the most prevalent related abuse (unauthorised disclosure or access) is indicative of two issues that *could* be addressed by more robust governance: 1) that *all* levels of staff that come into contact with or have specific roles handling health and biomedical data, do not have the proper training and/or incentive to handle data properly in keeping with the standards and procedures provided (or disincentives if they breach such standards or fail to follow procedures); *or* 2) the complete absence of *coherent* standards and procedures that guide staff clearly towards safe data handling and that address the specific situations encountered by staff at different levels of the organisation. However, there is a further and relevant difference between staff (training) failures and systemic failures. This distinction finds parallels between arguments and theories advanced in information governance literature that attempt to make sense of negligent practices within the NHS.

The absence of coherent standards and procedures was further apparent with regard to staff use of social media. As noted earlier,(news25) in 2011 there was a known lack of guidance for staff in this respect. In the interim, most Health Boards and Trusts have guidelines in place,[168] and the NMC [169] a guidance document.

Another case in point is the NHS, which featured especially prominently in the soft evidence strand (in forty-eight incidents out of sixty). Despite the arguably robust data handling protocols that for example NHS England operates under,[170] incidents of *repeated* and advertent abuse still occur. This could be explained by the ineffectiveness of training and/or

[168] For instance see: NHS England: http://www.rdash.nhs.uk/wp-content/uploads/2009/11/Social-Networking-approved-HROD-02.02.2012-V1.pdf; NHS Scotland: http://www.nhsaaa.net/media/132550/socmedpol.pdf; NHS Wales: http://www.wales.nhs.uk/sitesplus/documents/862/316socialnetworkpolicy.pdf.
[169] Nursing and Midwifrey Council, 'Social Networking Sites' (2012) http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Social-networking-sites/ accessed 29 April 2014.
[170] NHS England, 'Information Governance Policy' (2014) <http://www.england.nhs.uk/wp-content/uploads/2013/06/ig-policy-1.1.pdf> accessed 28 April 2014.

dissemination of standards and procedures when it comes to handing health or biomedical data.

An example of this is seen in the ICO's monetary penalty notice issued to North Staffordshire Combined Healthcare NHS Trust where several faxes containing sensitive health details of three individuals regarding their physical and mental health, special needs/mental health services provided and whether the individuals were at risk for self-harm, serious neglect or exploitation by others were sent mistakenly to a member of the public.[(ICOM4)] The mistakenly sent faxes were intended for the Wellbeing Centre (the "Centre") with remit to improving access to psychological therapies. Importantly in this case and to the assignment of maladministration as the cause for abuse, the ICO uncovered that:

- The Centre's new fax number was not pre-programmed into the NHS fax machine even thought that NHS office regularly sent faxes to the Centre. The Centre's fax number was input manually each time by staff, whereby in this incident, the fax number of the unintended recipient differed by one digit only.
- The NHS staff did not "call ahead" to the number, which could have flagged to them that the faxes were not received by the Centre.
- At the time of the abuse, this NHS office operated a safe haven policy and best practice guidelines that *were* available to staff via the NHS intranet. These guidelines provided that staff should pre-program the most frequently-used numbers into safe haven fax machines *and* operate a "call ahead" system.
- Importantly, the ICO found that the staff in question were not aware of the safe haven policy or best practice guidelines and did not receive any specific training relating to fax use. The ICO considered these shortcomings were exacerbated by a lack of effective management control.[(ICOM4)]

The implications that can be drawn from this example and instances of maladministration more broadly indicate a new approach to employee training - one that is contextualised not only to the role of the staff member (and thus appropriate to their level), but also one tailored to particular data handling practices such as email, fax, internet usage, patient intake, record keeping etc. (We discuss this further under 9.D.3.C Data protection awareness (re-)training – bringing home the real-life message) It is understood that many organisations operate information governance based on a one-size-fits-all training approach – the extremely high prevalence of abuse of data due to maladministration would seem to indicate that this approach should be re-visited.

In support of more contextualised training and guidance for safe data handling, specific incentives and/or disincentives for handling data according to proper protocol could further promote best practices. More robust methods for 'spot checking' data handling compliance could be considered as a means to combat complacency, laziness or outright disregard for

proper protocol. Furthermore, the disciplinary actions that result from abuses of data should be made clear in staff training, to *disincentivise* abuse (although and as we argue in 9.D.3 Disincentives, a soft approach can be crucial to the success of staff training – a dual approach can work very well in parallel). Finally, vigilance is required to ensure that best practices are in line with the current state of the art for technical security. Even if the loss of manual paper files was less prominent in the evidence, when digital copies of files are carried by staff off premises, high risks remain unless robust technical security measures are used and clear procedures are in place for what kind and how much sensitive health or biomedical data can be carried off premises (if at all).

How exactly robust technical security measures are maintained goes beyond the remit of this report. As an indication only, we list here: procurement should ensure that all devices purchased reach ISO/IEC 27001 standards,[171] the NHS IG Toolkit Administrator should ensure that he or she is up to date with latest developments,[172] and the Information Asset Owner must be able to provide assurance that 'the IG a) security risks have been considered and assessed on a regular basis, b) security measures have been implemented correctly and cannot be bypassed and c) security risks arising from use of the information asset are acceptable to their provider and other stakeholders.'[173]

9.A.2 Processing against individual objections or without their consent

Turning to a further prominent cause for abuse, we consider what form of consent (if any) is required when using the sensitive health or biomedical data of an individual for this has obvious implications for how data are governed within an organisation.

The use of personal or sensitive personal data, as defined in the DPA, must be justified on the basis of certain legitimising conditions under Schedule 2 of the DPA (if ordinary personal data) ***and*** under Schedule 3 if *sensitive* personal data – including health and biomedical data in the latter category. Despite the higher threshold for justifying the use of *sensitive* data, obtaining the consent of a data subject is ***not*** a strict requirement if other Schedule 2 and 3 conditions are met. Indeed, consent is neither necessary nor sufficient to comply with the provisions of the DPA. **This is a legal reality that escapes many, and it can lead to certain expectations about how data are appropriately handled.** Without speculating too far, such expectations can, in turn, lead to future feelings of affront or harm when consent has not been sought or obtained, and yet even when – notwithstanding – uses of data are perfectly legal and legitimate. It does not follow therefore that consent should always be sought. Rather these

[171] Information Standards Board for Health and Social Care, 'Information Governance' <http://www.isb.nhs.uk/use/baselines/ig> accessed 26 June 2014.
[172] Department of Health. 'BS ISO 27000 Series of Information Security Standards' <https://www.igt.hscic.gov.uk/isoiecsummary.aspx> accessed 26 June 2014.
[173] Note: Guidelines for NHS England. NHS Connecting for Health, 'NHS Risk Management' (2009) Appendix 4 <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/risk/inforiskmgtgpg.pdf> accessed 24 June 2014.

potential impacts should be appreciated and full(er) explanations or engagement put in place to address them and disabuse people of false assumptions and unjustifiable and untenable expectations.

In the hard evidence, incidents within this category were characterised as the use or proposed use of health or biomedical data against the stated objections of the individual(s); without fair notice; without obtaining consent; or, in cases where consent was refused. This cause of 'abuse' highlights the importance for data controllers to be able to distinguish between conduct that represents an *actual* breach of the law, and that, which may cause upset to some individuals but was technically lawful or permissible. If other conditions under the DPA justify a use of health or biomedical data simply because the individual did not consent to the processing, said use might still be lawful technically.

9.A.2.A Legal obligations and good governance

At this juncture, it is important to distinguish in context of the statements preceding this, the difference between the *lawful* use of health or biomedical data and the *good governance* of data, which will call for best practices that exceed technical obligations under the law.

In the hard evidence where health or biomedical data was/would be used against the wishes of individuals, this presents a strong case for better public engagement in the first instance, as opposed to indicating the need to obtain informed individual consent for each proposed data use. Good public engagement clarifies the boundaries for what could be done with an individual's data from the time of collection, boundaries that are maintained unless notice is given otherwise. Even when consent is obtained at a fixed point in time, a given use of health or biomedical data can still cause harm in future if new uses arise that change significant aspects of the transaction. A more reflexive, interactive relationship with individuals can help reassure that they *will* be given notice if anything changes significantly the way and purposes to which their data are used. Even when consent is infeasible to obtain or inappropriate under the circumstances (e.g. disciplinary proceedings or a disproportionately large number of individuals to contact), data controllers can promote robust public engagement, and give clear notice to what can be expected as to the data collected. It must be remembered that, due to advancements in medical knowledge and medical technologies, no-one can anticipate today how data might be used at a future date – another reason to have governance of the highest standards.

A full discussion on the nuances of operating on the basis of obtaining fully informed, individual consent for each proposed use of health or biomedical data, versus an opt-out clause, combined with fair processing notice(s) and good public engagement is outwith the scope of this report. However, it is important to highlight the distinctions made between what is legally required and that which is considered good governance or best practices. Importantly,

it is *not* the case that best practice would demand the need to obtain individual consent in all circumstances.

9.A.3 Unauthorised disclosure by the press

The incidence of press or media disclosing patient details without authorisation revealed a clear need for NHS staff and other organisations that handle sensitive health or biomedical data to have clear standards and guidelines governing interactions with the press. Such guidelines would need to be accessible and tailored appropriately for *all* levels of staff. There should be strong disincentives for breaching these rules. The liabilities of staff should be made clear when breaches of patient confidentiality occur, regardless of their position. Unauthorised disclosure by the press or media, facilitated by the lack of guidelines and/or implementation of proper protocol for hospital/medical staff speaking to the press, resulted in grave instances of harm to not only the individuals but also to their family and loved ones.

In *Armoniene v Lithuania*, decided by the ECtHR, a widow sought damages for financial harm and distress caused by the unauthorised disclosure of her husband's HIV-positive status by the press, as well as his affair with an HIV-positive woman that resulted in the birth of two extramarital children.(EUC5) The ECtHR detailed the grievous harm – both financial and emotional – caused to the entire family. The family were forced to move from their village after the information was published. The distress caused by the publication had a detrimental effect on the now deceased husband's health. The stigma associated with his HIV-positive status had a negative influence on his family life and restricted his family's ability to interact with the public.

In *P and another v Poland* a young woman was raped brutally and became pregnant.(EUC11) She made an early decision to have an abortion, but when seeking the procedure, the hospital issued a press release regarding her situation. The young woman became the centre of national news frenzy. She was harassed from unknown third parties, which forced her to be discharged from the hospital and seek treatment 500km from home.

Finally, in *Z v Finland*, the unauthorised disclosure by the press was in fact perpetuated by a Court of Appeals in Finland. It faxed a judgment to Finland's largest newspaper (*Helsingin Sanomat*) that confirmed a woman's HIV-positive status and disclosed her full identity.(EUC1) The ECtHR considered the damaging effect caused to Z's professional and personal life by this unnecessary disclosure by the Court of Appeal – with consideration of potential damage to wider public interests including the discouragement of '…persons from seeking diagnosis or treatment and thus undermin[ing] any preventive efforts by the community to contain the pandemic'; as well as damage to 'the interests of a patient and the community as a whole in protecting the confidentiality of medical data'.[174] Ultimately the ECtHR found the disclosure of the Court of Appeal's judgment to the press as unnecessary and awarded Z non-pecuniary

[174] *Z v Finland*, paras [96]-[97].

damages. *Z* v *Finland* highlights both the sensitivity of HIV-positive data, but also the care with which other professionals (lawyers, Courts, police) must and should treat such data.

Overall, the severity of harm caused by unauthorised disclosures by the press/media is indicative of the unstoppable trajectory that disclosed information disclosed takes in today's society. One need look no further than the recent Leveson Inquiry to confirm this.[175]

Once sensitive information regarding an individual's health is publicised and reported in the general media, the damage is no longer localised but capable of reaching even further audiences given today's digital society. Thus whilst *doctors* have a special relationship and thus obligation to maintain the confidentiality of their patients, it should be made clear to other staff within the health service, as well as other professionals including lawyers, police, courts, etc.) that they play a significant and important role in maintaining confidentiality (even if the direct line of legal liability does not necessarily fall with them).

This underscores again the need for on-going staff awareness training. Additionally, there is an increasing need for health care staff to be aware of blaggers, that is, those who knowingly or recklessly obtain or disclose personal data or information without the consent of the data controller. Such individuals are not only investigative journalists seeking to 'out' a public figure in some way. Indeed, the first blagging conspiracy came before the court in 2013.(Ti03) ICU Investigations Ltd with its three hundred and thirty strong client base of three hundred and thirty blagged personal patient details from (not only) GP surgeries. These details were then sold to clients (such as Brighton and Hove Council and Allianz Insurance) wanting to trace their debtors.

9.A.4 Unauthorised access due to insufficient safeguards

A case worthy of mention is that of *I v Finland*,(EUC9) which featured the unauthorised access of a woman's HIV-positive status due to insufficient safeguards being in place. In this case, a woman living with HIV and working as a nurse in Finland had paid regular visits to the same hospital's Infectious Diseases Clinic from 1987.[176] In 1992, the woman became suspicious that her colleagues were aware of her illness – at the time, hospital staff could access freely the patient register containing information on patients' diagnoses and treating doctors. Whilst, she did not claim that there had been any deliberate, unauthorised disclosure of her health data (it was not clear who may have accessed her health records), she did claim that the hospital failed to meet its obligation to keep her data secure against unauthorised access.

---

[175] 'Leveson Inquiry: Culture, practice and ethics of the press' <http://webarchive.nationalarchives.gov.uk/20140122145147/http:/www.levesoninquiry.org.uk/> accessed 29 June 2014.

[176] I v. Finland [2008] ECHR 20511/03 (17 July 2008); Big Brother Watch, 'Broken records: The worrying lack of security around your medical history, and how it is changing for the worse' (2012) <http://www.bigbrotherwatch.org.uk/brokenrecords.pdf> accessed 19 June 2014.

The ECtHR found in her favour, and awarded her compensation for the distress caused by the need to change her employment and the effect of the rumours on her son's life.[177] It is worth noting that the woman also claimed for financial damages relating to her contract not being renewed and her needing to move homes because of the rumours surrounding her health. Although her financial loss was not recognised legally (due to insufficiency of causal evidence), it nevertheless highlights the serious and wide-ranging *impacts* that abuse of health data can have. Importantly, the ECtHR found that:

> Although the object of art 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life.[178]

This indicates the important *positive* obligations data controllers have, to ensure proactively technical and organisational safeguards are in place, to secure the personal health data they hold.

9.A.5 Human error

Human error was also a key issue uncovered in the evidence and is well recognised by the ICO: in the first quarter of 2013, more than half of the data breach incidents reviewed by ICO were caused by human error (down to the carelessness of individuals handling the data).[179] Incidents caused by human error such as misplacing an unencrypted USB stick somewhere at work(ICOM2) or leaving behind sensitive documents on a train(ICOM7) could at least be *partially* resolved by better employee training and technical barriers to staff downloading especially sensitive data to portable devices. The evidence would suggest a relationship between cases of human error and maladministration, or in some cases an interaction between the two. Additionally, these two causes were often 'borderline', whereby a judgment was made to assign a single cause. In cases where the abuse was a one-off occurrence and, on the face of the evidence, not indicative of a systemic issue of poor data handling, human error was assigned. Ultimately, this category represents the unknown and unchangeable element in the risks of handling sensitive data, that is, the human element – one that the ICO acknowledges as a key cause for data breach incidents.[180]

It is also useful to consider at this point unintentional human error in the context of the healthcare workplace and working conditions. The NHS across the UK is in dire financial

[177] *I* v *Finland*, para [53].
[178] *I* v *Finland*, para [36].
[179] Sally-Anne Poole, 'ICO blog: The cost of carelessness - how stats help inform the action we take' (ICO, August 2013) <http://ico.org.uk/news/blog/2013/the-cost-of-carelessness-how-data-informs-the-action-we-take> accessed 29 April 2014.
[180] Sally-Anne Poole, 'ICO blog: The cost of carelessness - how stats help inform the action we take'.

straits, and staff workloads are increasing exponentially.(BBC01,H03,Te20) In times of stress, the risk of carelessness increases.

In addition, we see the first steps towards integrated care in the UK, where health and social services data will be linked. As Goodwin, Smith and colleagues note, 'governance needs to be aligned across the various health and social care providers to drive shared interests and accountability in care delivery for people'.[181] The workforce accessing health and social care data will increase, an array of IT systems and platforms will be communicating, and each linked organisation will come with its own culture, priorities and IT knowledge-base. It is therefore vital that information governance is developed appropriately and rigorously alongside other pathways to integration.

Overall, despite the existence of robust data handling procedures, there always remains the possibility for human error to intervene. Human error represents one of the causes identified that should be distinguished from more intentional and flagrant abuses of health or biomedical data, given the inadvertent nature of these abuses.

9.A.6 Falsification and fabrication

It could be argued that falsification and fabrication, such as the cases identified in the newspaper search (and single case in the hard evidence(UKC9)), are less a question of good governance and more a question of criminal intent. It goes beyond the remit of this review to discuss this in full. However, if cases of falsification and fabrication of health or biomedical data fall within the remit of the ICO, then custodial sentences are not, we argue, too harsh. Indeed, Christopher Graham, the Information Commissioner, has been pressing government for tougher penalties.(Te12)

We differentiated earlier between the individual perpetrator and serious management failings that have led to falsification and fabrication, and discussed these in depth in Section 7.B.2.B.1 Impact of harm caused through falsification/fabrication. Whereas the individual (presumably) acts alone or with a few other individuals, falsification and fabrication on a larger scale involves perpetrators and those who may be considered 'guilty by association' – or at least witnesses to such abuse. The question remains as to why it is difficult to combat falsification and fabrication in the NHS despite the clear existence of proper data handling protocols. One possible answer lies in the fears that staff might harbour after whistle blowing or where the work environment is that of harassment and bullying. Another possible answer lies in the perceived need for some middle and senior NHS management to meet organisational targets.

[181] Nick Goodwin et al, 'Integrated care for patients and populations: Improving outcomes by working together' (The King's Fund and Nuffield Trust 2012) <http://www.nuffieldtrust.org.uk/sites/files/nuffield/publication/integrated_care_for_patients_and_populations_-_improving_outcomes_by_working_together_jan12_0.pdf> accessed 18 June 2014.

We differentiated earlier between the individual perpetrator and serious management failings that have led to falsification and fabrication. Whereas the individual (presumably) acts alone or with a few other individuals, falsification and fabrication, on a larger scale, involves perpetrators and those who may be considered 'guilty by association' or at least witnesses to such abuse. The question remains as to why it is difficult to combat falsification and fabrication in the NHS despite the clear existence of proper data handling protocols? A possible answer lies in the fears that staff might harbour after whistle blowing or pressures to meet organisational targets.

9.A.7 Genetic data

The only case uncovered in the search for genetic data was *S and Marper v United Kingdom*,(EUC7) which focused on an alleged interference with the applicants' Article 8 rights to respect of private life under the European Convention on Human Rights.[182] The implications arising from the abuse of *genetic* data warrants discussion along with the important issues raised by this case. Furthermore, Section 10 *Future Research* will highlight abuse of genetic data as an area warranting further research.

9.A.7.A S and Marper v United Kingdom

This case featured a long history of trial domestically, before escalating to its review by the ECtHR.[183] The two applicants, "S" and Michael Marper, were both previously arrested, whereby S was eventually acquitted at trial and the charges against Marper were dropped. Despite this, and in keeping with (then current) police policy in the UK,[184] their DNA profiles, "cellular samples"[185] and fingerprints were to be retained without any stipulated time for disposal. The applicants applied to the ECtHR to seek destruction of their DNA profiles, cellular and fingerprint samples as they contested it was a violation of their Article 8 rights to respect of private and family life.

In considering the case, the ECtHR considered the nature of DNA profiles, cellular samples and fingerprints, and specifically, each of the data/material's propensities to reveal sensitive information about S and Marper. The Court distinguished between cellular samples on the one hand and DNA profiles on the other:

---

[182] S and Marper v United Kingdom (2009) 48 EHRR 31.
[183] *R v Chief Constable of South Yorkshire* [2004] UKHL 39 [7], [2004] 4 All ER 19 on appeal from [2002] EWCA Civ 1275 and [2002] 1 WLR 3223.
[184] Section 64(1A) of Police and Criminal Evidence Act 1984 (as modified by Section 82 of the Criminal Justice and Police Act 2001) authorised police in England and Wales to retain collected fingerprints or DNA samples so long as they were only used in relation to preventing or detecting crime, investigations of an offence or in prosecutions. The provisions governing retention of samples in Northern Ireland were identical to those in England and Wales, whereas in Scotland samples must be destroyed if the individual is either not convicted or fully acquitted (bar certain crimes, and then a three-year retention period applies). 1995 Criminal Procedure Act of Scotland, s 18(a).
[185] The ECtHR refers to cellular samples (rather than DNA samples) to mean what we presume are the blood, semen, saliva or hair samples taken from S and Marper at the time of their arrest.

> DNA samples are cellular samples and any sub-samples or part samples retained from these after analysis. DNA profiles are digitised information, which is stored electronically on the National DNA Database together with details of the person to whom it relates.[186]

Of relevance to this report are the DNA profiles, as representative of the digitised information (or *data*) stored after analysis of the samples. Whilst cellular *samples* are technically outwith the scope of this evidence review (as the remit of this report is related to health and biomedical *data*) the implications arising from the Court's discussion over DNA samples is nonetheless important to our understanding of the implications arising out of abuses of genetic data. The Court considered DNA profiles and cellular samples together, although reaching different conclusions as to the relative sensitivity of each.

As to cellular samples, the Court found the applicants' concerns legitimate – specifically as to potential future abuses:

> An individual's concern about the possible future use of private information retained by the authorities is legitimate and relevant to a determination of the issue of whether there has been an interference. Indeed, bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today.[187]

The Court acknowledged the pace of technological advancement was such that S and Marper held legitimate fears as to future, intrusive surveillance to which they could be subjected. However, this was not the only consideration – the Court found particularly sensitive, the data cellular samples could reveal about both an *individual's* health as well for their relatives.[188] This is in agreement with the NCOB report on bioinformation that was cited to in this judgment[189] whereby cellular (DNA) samples (containing entire genetic sequences of individuals) are recognised as holding serious potential for revealing ever more sensitive personal data regarding an individual's health, family relationships, and potentially even behaviour.[190]

---

[186] S and Marper v United Kingdom [footnote 1].
[187] S and Marper para [71].
[188] Thus the *data,* which could be produced from analysing the samples, was what was most sensitive. *S and Marper* para [72].
[189] The ECtHR noted the NCOB's concerns regarding indefinite retention of bioinformation such as to the "lack of satisfactory empirical evidence to justify the present practice of retaining indefinitely fingerprints, samples and DNA profiles from all those arrested for a recordable offence, irrespective of whether they were subsequently charged or convicted." See *S and Marper* paras 38-40.
[190] The Nuffield Council on Bioethics, 'The forensic use of bioinformation: ethical issues', September 2007 para 1.12.

The Court then considered DNA profiles. Despite the fact that DNA profiles contained 'a more limited amount of personal information extracted from cellular samples in a coded form', the Court found that nonetheless 'the profiles contain substantial amounts of unique personal data'.[191] This is in accordance with the NCOB report on *Bioinformation* that provides that DNA profiles do not in themselves reveal a substantial amount of personal data bar (potential) identification and gender.[192] Nonetheless, the ability for the police and authorities to use DNA profiles to conduct a) familial searching to identify genetic relationships between individuals and b) make inferences regarding an individual's ethnic origin was considered extremely sensitive and impactful on private life.[193]

As such, the ECtHR found that a) the retention of DNA profiles, cellular samples and fingerprints[194] sufficiently related to the applicants' private lives under Article 8 and b) that the indefinite retention was a 'disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society'.[195] This was despite the Court's acknowledgement that the United Kingdom *was* serving a public interest, in the prevention crime.

This ruling holds great implications for *widening* the *legal* notion of harm (at least in relation to Article 8 considerations[196]). The *potential* for the DNA samples to be used in a discriminatory fashion in future (and cause harm), with special consideration of the potential impact on the younger "S" (who at the time of arrest was eleven years old), skewed the evidence *in favour* of the applicants. The weight given to the *potential* to cause harm, in light of future advancements in DNA analysis, highlights the broad implications that arise with the use, or mere storage of genetic data. However, the public interest in protecting the privacy in genetic data, data which may reveal information about an individual's health, or even information that he or she might not have been aware of (e.g. familial relationships) will often be balanced against *other* public interests, such as those served through its utility in crime detection and prevention.

In the now successfully appealed House of Lords judgment *R (on the application of S) v Chief Constable of South Yorkshire R (on the application of Marper) v Chief Constable of South Yorkshire* in 2004, the Court considered that '[t]he value of retained fingerprints and samples

[191] *S and Marper* para [74]-[75].
[192] This is explicitly recognised by the ECtHR in *S and Marper* as well as by the NCOB in The Nuffield Council on Bioethics, 'The forensic use of bioinformation' paras 1.12 and 4.53.
[193] *S and Marper* paras [75]-[76].
[194] The ECtHR held that fingerprints were sufficiently related to S and Marper's Article 8 rights to private life, albeit that DNA profiles and cellular samples had a more important impact on their rights. Specifically, the Court held that the retention of their fingerprints 'on a nationwide database with the aim of being permanently kept and regularly processed by automated means for criminal-identification purposes' was sufficient to be deemed an interference with said rights. *S and Marper* para [86].
[195] *S and Marper* para [125].
[196] Which are arguably broader than those permitted under UK data protection law or even common law.

taken from suspects who were subsequently acquitted is considerable'.[197] The major role DNA evidence played in the detection and prosecution of serious crime was the proper context in which the indefinite retention of S and Marper's DNA samples, profiles and fingerprints would be assessed under human rights law.[198] Opposite to the judgment of the ECtHR, the House of Lords considered:

> [F]ears of what may happen in the future in the light of the expanding frontiers of science [are] not relevant in respect of contemporary use of retained samples in connection with the detection and prosecution of crime. If future scientific developments require it, judicial decisions can be made, when the need occurs, to ensure compatibility with the convention.[199]

The House of Lord's finding that the indefinite retention of DNA samples, profiles and fingerprints as only *modestly* interfered with S and Marper's private lives,[200] lies in stark contrast to the broad perspective taken by the ECtHR; a perspective which would eventually cause a change to such laws in the UK.[201] The House of Lord's treatment of the issues around retention of genetic data emphasise the narrowness taken to considerations of 'harm' in the UK context, even when operating within the remit of human rights law and in particular Article 8.

This divergence of judgments also importantly accentuates the variable quality of public interest judicial determinations – in the House of Lords case, the public interest factors weighed *against* S and Marper in finding indefinite retention both legitimate and proportional to any modest interference with their Article 8 rights. This is the precise opposite to the ECtHR case where the balance was skewed *in favour* of S and Marper as the *indefinite* retention of their DNA profiles, samples and fingerprints were found to substantially interfere with their Article 8 rights to private life *and* the interference was disproportionate to the legitimate aim sought (prevention and detection of crime). Thus, there is likely to be no legal certainty when public interests are balanced – it will be on the facts of each case to determine where the balance lies. Even though the search for 'genetic data' uncovered only one case, it is a case of

---

[197] *R v Chief Constable of South Yorkshire* [2004] UKHL 39 [7], [2004] 4 All ER 19.
[198] [2004] UKHL 39 [8].
[199] [2004] UKHL 39 [28].
[200] [2004] UKHL 39 [32].
[201] In response to the ECtHR's ruling in *S and Marper*, the UK amended its legislation (via the the Protection of Freedoms Act 2012) to require the destruction of obtained DNA samples, profiles and fingerprints after a specified period of time and subject to relevant conditions based on the status of the conviction, previous convictions, age, etc. The changes regarding *destruction* of data are found under the Police and Criminal Evidence Act 1984, ss 64ZA–64ZJ, with changes regarding retention and use of material, in ss 64ZK–64ZN of the Act. Scotland already had provision for destruction of samples within certain time limits and under certain conditions. In 2011, Northern Ireland's Justice Minister proposed changes to legislation in light of *S and Marper* but to-date this consultation has yet to be implemented – in fact in late 2013 the Justice Minister launched a new DNA database system whereby a 'DNA profile can be obtained from just one or two human cells and from areas where it would not have been possible before.' 'Justice Minister Launches Improved DNA Profiling Service' (*Northern Ireland Executive* 2013) <http://www.northernireland.gov.uk/news-doj-121213-justice-minister-launches> accessed 23 June 2014.

importance – one that broadened the legal landscape to recognise and provide for new notions of harm as they relate to genetic data and samples. For S and Marper, the public interest balance did lie in favour of protecting the privacy in their genetic data and DNA samples. As such, this perpetuated an important change to the law in England and Wales where samples must be destructed under certain conditions and timescales.

Overall, the ECtHR case of *S and Marper* serves as a reflection on the range of potential harms that can arise from mere storage of genetic data, whereby it is the *informational value* of *analysed* DNA samples that can impact upon individuals' right to respect of private life. The case crucially serves as a reaffirmation of the importance of considering harm outwith the narrow scope of *actual* harm (as understood in legal terms) both when planning and implementing good governance of health and biomedical data. The unique capability of *genetic* data to identify, characterise and speak to physical, physiological, familial qualities and relationships ensures that its use or mere storage will give rise to a host of ethical and legal considerations.

9.A.8 Non-use of data

9.A.8.A Focus of this section

As well as harms resulting from the abuse of biomedical and health data, there are the effects due to non-use of such data to consider. However, it is acknowledged that little/no actual evidence of harm due to the non-use of data was found by the searches used in this review, and that it would be challenging at best to determine with a high degree of confidence whether an instance of harm was truly due to the non-use of data, or whether its causes were otherwise in the presence or absence of adequate data. It is also important to retain the distinction between harm due to the non-use of data and the benefits due to the use of data, and not to simply invert the latter and effectively equate the two. It could be misleading and inaccurate to postulate that benefits resulting from the use of data in a study would not have been realised, and that the opposite outcomes would have occurred, if those data had not been used. Therefore, this section will identify and discuss some important reasons for the non-use of data, with examples of consequences or lost opportunities where available, to help clarify why problems due to the non-use of data are not more evident.

9.A.8.B Context

It is universally accepted that data collected in the course of healthcare delivery hold great potential for research and the improvement of clinical practice and patient care if they can be made available as needed. The traditional position within the UK is of data in silos, such that GP data is held within the practice and not systematically shared with hospitals, and even within a given hospital, data are held on administrative or departmental systems that may communicate with each other to varying extents. Valuable data collected for research might not be put to any further use after the end of the study. The question arises as to why the

wealth of routinely-collected and bespoke study data are not being used to best advantage. Whilst the complexities and constraints of the various legislative and regulatory governance frameworks are undoubtedly relevant here, it is worth reviewing other, some rather fundamental, factors at play in the non-use of data. To do this, we need to take a step back.

9.A.8.C Clinical records

In 1996, the National Audit Office (NAO) published a report entitled '*Setting the Records Straight*'[202] and this noted numerous problems with paper case note keeping. Among the hospitals studied, 12 of the 16 kept multiple sets of casenotes for some patients, which could lead to confusion in administering care. Among 121 clinics, only two-thirds of casenotes were at hand for immediate use, and although most were located in adequate time, on some occasions (up to 3%) the search was fruitless and the patient was unable to receive their consultation. This has serious implications for the continuity of patient care, and may force a delay in surgical procedures because patient history cannot be verified. It carries professional risks to the duty of care of the clinical team in not being able to make informed decisions. It also imposes an unnecessary financial burden due to wasted time for staff and patients. Missing casenotes can bias clinical audit, thus skewing the information used to monitor and advance clinical practice. For example, an audit of antenatal risk factors found that 6.4% of the casenotes were missing. Although this sounds like a relatively small proportion, the suggestion was that this was non-random as clinicians tended to hold onto interesting cases for research or further discussion.[203] As well as entire case notes going missing, individual test and procedure results, and sometimes episodes of care can be missing from the file. This again may delay timely care leading to poorer outcomes and subject the patient to duplicate risky invasive processes. It also wastes public money and staff time.[204]

Since this particular NAO report was published 18 years ago, there have been considerable advances in the use of electronic clinical systems in healthcare. Nevertheless, we are still a long way from having a comprehensive electronic patient record, let alone being able to use and share it effectively. Swansea University hosts the UK Multiple Sclerosis (MS) Register.[205] When the Register was being established in 2009, we carried out a survey of clinical record-keeping methods in NHS Neurology clinics across the UK. Of the 47 respondent clinics, 5 still used only paper records, 8 stated that they used a word processor package, and only 10 said they used an MS-specific clinical system.[206] We had to take purposive action in

[202] National Audit Office, 'Setting the record straight' (1995) <http://archive.audit-commission.gov.uk/auditcommission/subwebs/publications/studies/studyPDF/1134.pdf> accessed 18 June 2014.
[203] A F E Yoong, C Hudson and T Chard, 'Medical audit: the problem of missing case-notes' (1993) 25:3 Health Trends.
[204] National Audit Office, 'Setting the record straight'.
[205] David Ford et al, 'The feasibility of collecting information from people with Multiple Sclerosis for the UK MS Register via a web portal: characterising a cohort of people with MS' (2012) 12:1 BMC Medical Informatics and Decision Making, 2012,12(1):73 (18 July 2012).
[206] Rodden M Middleton et al, 'Clinical system usage in NHS Specialist Neurology sites' (RIMS conference, Brighton, June 2014).

order to facilitate data collection for the MS Register, and we adapted an open-source clinical system and made it available to our participating sites. There doesn't seem to be any reason to assume that Neurology is different to other disciplines and so the significance of this is that the pace of change towards electronic systems is slow, and that without the use such systems, the effective use of medical and health data is hampered. The primary task of NHS staff is to deliver patient care, and with the high service demand that exists, even with the best will in the world, staff are limited in the effort they can dedicate to other pursuits without sufficient funding, training and time.

Even when a clinical system is in place, there are issues that impact on data availability for use. A team of healthcare professionals may be involved in an episode of care, some of whom may enter data into the system, and some of whom may record data on paper to be transcribed later by an administrator. Although it may never be intended that every piece of information should reside in the electronic system, this does introduce the possibilities of error and non-entry of important data. It is also the case that when an electronic system is implemented, a judgement call has to be made on the bases of relevance and resources as to how much back data is entered into the system. Thus there are issues of data quality and completeness within individual systems to contend with before we consider system interoperability so that information from different systems can be combined. Without this, the data are still in silos, albeit now electronic ones.

Among the classic difficulties in data compatibility are differing formats and data structures, which may inhibit data integration, and different coding systems that limit semantic interoperability. For example, primary care services often use Read codes to record diagnoses,[207] whereas hospital settings often use the International Classification of Disease (ICD) nomenclature.[208] This means there would have to be a form of translation in order to interpret information from one system to another in seeking to provide the best patient care. There is a move to standardise coding systems to promote interoperability by means of the Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT), which provides a comprehensive clinical terminology. It has been adopted in over 50 countries, and is the approved system for NHS England.[209] It will undoubtedly take considerable financial resource, time and effort to introduce a more standard coding system, but it essential that information is consistent and transferable if data are to be used optimally for individual patient care and, beyond that, to maximise their usefulness in studies for wider benefits.

[207] Health and Social Care Information Centre, 'Read Codes' <http://systems.hscic.gov.uk/data/uktc/readcodes> accessed 18 June 2014.
[208] World Health Organisation, 'International Classification of Diseases (ICD)' <http://www.who.int/classifications/icd/en/>accessed 18 June 2014.
[209] Health and Social Care Information Centre, 'SNOMED CT' <http://systems.hscic.gov.uk/data/uktc/snomed> accessed 18 June 2014.

9.A.8.D Research data

The concept of wider benefits leads us to consider factors that influence the non-use of data in research studies. Though the impacts of research are not immediate, in that it takes time for findings to be translated into policy and practice, the non-use of data in research can have far reaching effects on patient care, the healthcare profession and the economics of the NHS. Again, the issue of data absence within clinical systems is an obvious cause of data non-use through non-availability. A study of 10,000 electronic health records in New York found that the selection process whereby researchers naturally aim for data completeness can result in systematic bias. This is because sicker patients tend to have a higher degree of data sufficiency within their records. It is a problem characteristic of studies relying on the secondary use of data, since data items resulting from tests and procedures are just not present for healthy individuals. Unless this is taken into account, the findings will not represent the population from which the sample was drawn as they will over-estimate the problem and limit external validity.[210] This is the converse of the problem identified in the antenatal clinical audit (above),[211] where some of the problematic cases were excluded, thus underestimating the extent of issues to be addressed. Either way, the findings could be misleading and lead to sub-optimal recommendations, but unless individual cases could be obtained, examined and followed through, it would not be meaningful to discuss harm due to the non-use of data. Even then, it would be challenging to show cause and effect if a case was brought to litigation.

Before considering the governance landscape and its influence on data use, it is worth exploring some of the other reasons researchers and organisations may or may not choose to share their data. Within the non-commercial sector, the majority of substantial research takes place in academia. Researchers may invest extensive time, energy and intellectual input into gathering, collating and analysing datasets, and there are still little in the way of incentives for sharing data.[212] They may also be under immense pressure to produce high impact outputs for the Research Evaluation Framework (REF). It is arguable whether this is an ethical practice, since it influences the research that is carried out and what is ultimately published. Publication bias is a well-known phenomenon with weaker or negative findings less likely to make it to the journals. Biomed Central has established the Journal of Negative Results in Biomedicine to publish 'unexpected, controversial, provocative and/or negative results in the context of current tenets'.[213] But an impact factor of 1.15 offers little kudos, and so as long as the expectation of the REF persists, it's likely that many researchers will have to concentrate their efforts on hitting their targets. As a result, publication bias will remain a source of data non-use

[210] Alexander Rusanov et al, 'Hidden in plain sight: bias towards sick patients when sampling patients with sufficient electronic health record data for research' (2014) 14:51 BMC Medical Informatics and Decision Making.
[211] A F E Yoong, C Hudson and T Chard, 'Medical audit: the problem of missing case-notes'.
[212] Expert Advisory Group on Data Access 'Establishing incentives and changing cultures to support data access' (2014) <http://www.wellcome.ac.uk/About-us/Policy/Spotlight-issues/Data-sharing/EAGDA/WTP056496.htm> accessed 18 June 2014.
[213] 'About Journal of Negative Results in Biomedicine' <http://www.jnrbm.com/about> accessed 18 June 2014.

and studies with undesirable findings may be repeated. The resulting waste of time and effort represents an opportunity cost as public money could be better utilised and needless duplicative intrusion into patients' lives could be avoided.

The commercial sector invests billions in drug development and clinical trials. Taking into account the high failure rate in drug creation, it is estimated that it costs approximately $5 billion to bring a new drug to market.[214] As well as seeking the best treatments for patients, pharmaceutical companies are obviously concerned with generating income and protecting their intellectual property. As a result, the information they release about drugs may be biased as it is selected to maintain and extend their market share. In his book '*Bad Pharma: how medicine is broken and how we can fix it*', Ben Goldacre states that is it beyond doubt that 'industry-funded trials are more likely to produce positive, flattering results than independently-funded trials'.[215] For example, it is cited in a 2010 review of trials that 85% of industry-funded were positive, but this was the case in only 50% of government-funded trials. A variety of reasons are proposed for this higher rate of apparent success including: not publishing unflattering results; comparing a new drug against a placebo, or against an inadequate drug at too low a dose; selecting patients without proper randomisation; or using small, specific sample groups.[216]

There have been some devastating examples where non-use of data due to non-publication of research findings has been linked to harm to individuals. There was a particularly high-profile example in 2006, in a first-in-man trial of an immune-modulatory drug referred to as TGN1412. Six healthy volunteers were administered with the drug and within an hour they began suffering horrendous side-effects. The Department of Health convened an Expert Advisory Group to investigate the situation and develop recommendations to try and prevent similar occurrences. The final report concluded that new experimental treatments should not in future be given to all the volunteers at the same time, but in response to the question of whether the situation could have been avoided, it transpired that there had been some experience with a similar intervention ten years previously. A researcher presented the inquiry with unpublished data relating to the use of an antibody molecule with parallel effects in a single human subject. No one could have foreseen the significance of this unpublished piece of information, but the final report recommended that the results of every first-in-man trial should be made available to avoid a repeat of the terrifying ordeal to which the six volunteers were subjected. However,

[214] Matthew Herper, 'The Cost Of Creating A New Drug Now $5 Billion, Pushing Big Pharma To Change' (*Forbes*, 2013) <http://www.forbes.com/sites/matthewherper/2013/08/11/how-the-staggering-cost-of-inventing-new-drugs-is-shaping-the-future-of-medicine/> accessed 18 June 2014.
[215] Ben Goldacre, Bad Pharma: how medicine is broken and how we can fix it (Fourth Estate publishers 2013).
[216] Ben Goldacre, *Bad Pharma*.

a review conducted in 2009 showed that the majority of these Phase 1 trials were still not being published, allowing this form of data non-use to continue.[217]

Another example of harm to patients through non-publication of data can be seen in the use of an anti-arrhythmic drug administered in the 1980s to patients who had suffered a heart attack. It is estimated that over 100,000 patients died of a heart attack after taking the drug before it was realised that it was not appropriate for people who did not have arrhythmia. As to whether this disastrous situation was avoidable, it transpired that a small study had been carried out in 1980 in which 9 of 48 men who took the anti-arrhythmic drug (lorcainide) died, compared to 1 of 47 taking the placebo. As a result, the drug was dropped for commercial reasons and the findings were not published. Over a decade later the researchers did publish and stated that their results might have provided an early warning.[218]

Sometimes there are direct accusations that data have been withheld to the detriment of patients. One such example concerns a private company, by the name of Myriad Genetics, which specialises in testing for genetic variants linked to breast cancer. When a mutation is found, counselling is offered to the patient and family members concerning their risk status. Although Myriad has access to public databases, it has refused to share its data on the grounds of it being proprietary information. Thus Myriad retains its market advantage but vital information is being withheld. It is also reported that this occurs with other genetic testing companies and the practice, though immoral is not actually illegal. This is an example of where the legislative and regulatory frameworks are lagging behind scientific developments and action needs to be taken to address these scenarios.[219]

9.A.8.E Governance frameworks

This brings us to consider the impact of governance frameworks on the non-use of data. These have long been blamed for hampering the use of data and hindering research. Criticisms have been levelled at particular pieces of legislation or regulations, but also at subjective interpretations resulting in over-cautious implementation and unnecessary bureaucracy. This may include lengthy forms and approval processes, unnecessary steps and parties involved in approval procedures, over-stringent rules on data access, and the lack of clear responsibilities delaying permissions, amongst other obstacles. In the past ten years, vast amounts of effort have been put into streamlining the regulatory and governance landscape and in providing better information to researchers. Even so, the current and proposed frameworks can present huge challenges to the use of data, not only for research, but also for service and care planning. It is a commonly held belief among the public that

[217] Evelyne Decullier, An-Wen Chan and François Chapuis, 'Inadequate Dissemination of Phase 1 trials: a retrospective cohort study' (2009) 17:6(2) PLoS Medicine.
[218] AJ Cowley et al, 'The effect of lorcainide on arrhythmias and survival in patients with acute myocardial infarction: an example of publication bias' (1993) 40:2 International Journal of Cardiology.
[219] Nigel Hawkes, 'Genetics testing firm is accused of "hiding vital breast cancer data"' (*BMJ News*, 2012) <http://www.bmj.com/content/345/bmj.e7402> accessed 18 June 2014.

healthcare and government administrative data are already linked and shared across services.[220] However, of course, this is not the case, as data cannot even be passed from one sector of the health service to another without justification and permission.[221] This means there is great potential for medical error through lack of joined-up information. For example, hospital patients are usually asked if they are taking any medication before they are treated, whereas their primary care record could be reviewed if it were accessible. A similar process occurs with other practitioners such as dentists before they prescribe. Medication errors are the single most common preventable cause of adverse event in medication practice,[222] and it is easy to argue that more joined-up information could circumvent at least some of these occurrences.

But individuals may not find combining and sharing identifiable data with other practitioners acceptable without their agreement, and the governance frameworks that exist serve to safeguard individual rights to privacy. In order to make use of personal data, it is necessary to obtain regulatory approvals, which often require informed consent of the individuals concerned. This is an established part of research ethics and governance frameworks.[223] However, it can be argued that, in some cases, the pursuit of informed consent can disadvantage certain groups, particularly those who are hard to reach or on the edges of society. It has been proposed that this is the case in seeking to solve '*wicked*' problems often associated with the youth, such as psychosocial issues, school failures and drop-outs, risk-taking behaviours, substance misuse and juvenile crime. A powerful argument can be made that, as such problems require the best data, insisting on consent is a failure of duty.[224] A similar argument in relation to bias due to consent was evidenced by comparing baseline and follow-up data from GP and hospital records on patients who did, with those who did not, consent to an intracranial malformation study. The results showed that consenters were systematically different in ways that could not have been estimated in advance. The authors concluded that those who oversee medical research are harming public health by imposing greater constraints on patient data than those required by the law.[225]

This problem of not being able to use non-consented data is not limited to research but also impacts upon patient care, and it is proposed that sharing data across the health and care system could save lives. A case in point was that of a vulnerable little boy who died in 2011 following systematic abuse. There were interactions with, and reports to, various health and

[220] Ipsos MORI Social Research Institute 'Dialogue on data' (2014) <http://www.ipsos-mori.com/researchpublications/publications/1652/Dialogue-on-Data.aspx> accessed 18 June 2014.
[221] As regulated by the DPA.
[222] European Medicines Agency, 'Medication Errors' <http://www.ema.europa.eu/ema/index.jsp?curl=pages/special_topics/general/general_content_000570.jsp> accessed 18 June 2014.
[223] 'Health Research Authority' <http://www.hra.nhs.uk/>accessed 18 June 2014.
[224] Fiona Stanley, 'Privacy or public good? Why not obtaining consent may be best practice' (2010) 7:2 Significance 72-75.
[225] Clare Dyer 'Stringent constraints on use of patients' data are harming research' (2007) BMJ 1114-1115.

social care providers, but the data were isolated and the problems were not identified in time. Furthermore, the article states that too much emphasis is placed on the risks of implementing data sharing initiatives, rather than on the potentially enormous risks of not making data available.[226] This perspective is not limited to the UK, but it accords with opinion from elsewhere. For example, a report from the US states that the non-use of patient clinical data is a greater risk than abuse, such that:

[T]he greatest threat, the biggest risk to people with diabetes, or heart disease, or cancer, or HIV/AIDs or any other chronic disease or disability seems not to be from un-authorized sharing or use of their personal health information, rather it is from the failure to share or the inadequate use of that information, and sometimes even valuing protecting privacy over protecting an individual's life, their health, and the health of their families, friends and neighbours.[227]

Within the UK there are specific, regulatory mechanisms that permit the use of identifiable, patient data, without consent in certain circumstances. There is provision for the common law duty of confidentiality to be over-ridden for important medical and research purposes was made possible via section 251 of the NHS Act 2006.[228] Applications are administered by the Confidentiality Advisory Group of the Health Research Authority,[229] but at least anecdotally, the success rate is low and applicants are strongly encouraged to pursue the consent route or to use anonymous data where at all possible. In some cases, this does not compromise the purpose, but in others, it does. But there are many success stories; for example, the author of this section is engaged in a study of vulnerable young mothers and their children that has successfully obtained s251 support. Without this, the study would have been biased since the participants could not be followed-up reliably. Even so, the waiver was only granted for matching purposes, that is, so that the study data could be linked to hospital and education data, and it was a condition of the approval that the resulting de-identified data had to be accessed via a Safe Haven.

The Information Governance Review published in 2013, commonly referred to as Caldicott 2, includes an additional recommendation compared to the first Caldicott report. This is that the duty to share information can be as important as the duty to protect patient confidentiality.[230] It also includes considerable discussion on Safe Havens as 'specialist, well governed,

[226] Gareth Iacobucci, 'Sharing care data could save lives of vulnerable children, hospital leader says' (*BMJ News*, 2014) <http://www.bmj.com/content/348/bmj.g1953> accessed 18 June 2014.
[227] David St. Clair, 'Non-use of Patient Clinical Data a Greater Risk than Misuse' (*Managed Healthcare Executive*, 2008) <http://managedhealthcareexecutive.modernmedicine.com/managed-healthcare-executive/news/non-use-patient-clinical-data-greater-risk-misuse?page=full> accessed 18 June 2014.
[228] NHS Act 2006.
[229] Health Research Authority, 'Section 251 and the Confidentiality Advisory Group (CAG)' <http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/#sthash.mIuhDEoq.dpuf> accessed 18 June 2014.
[230] Department of Health, 'Caldicott review: information governance in the health and care system' (2013) <https://www.gov.uk/government/publications/the-information-governance-review> accessed 18 June 2014.

independently scrutinised accredited environments' as the sole location where the linkage of personal confidential data from more than one organisation for any purpose other than direct care, should only take place. This helps to highlight the innovative work that has been underway for some years on the development of Safe Havens for access to de-identified linked data for research. The SAIL system is one such example where approved researchers can access data for research within a secure environment.[231] However, although Safe Havens hold great promise for using the wealth of valuable, extensive health-related datasets, they are still subject to limitations. Not least among these is the constraint of using only de-identified data. Many types of study don't require identifiable data to produce benefits, as proven by the rich array of important research outputs produced via anonymous data linkage research; a good example being work conducted via the long-established Western Australia data linkage unit.[232] But de-identified data are not exempt from privacy protection measures and these may affect the granularity of the data researchers can access and so impact on research findings. This is relevant in the context of this report because it is a form of data non-use.

The DPA defines personal data as 'data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.'[233] The alternative is to use anonymised data, and there are various viewpoints on what actually constitutes anonymous data. It has been established that individuals can sometimes be re-identified from data purported to have been anonymised.[234] Because of this, it is good governance practice that de-identified data are curtailed before being made available for research. This may take the form of aggregation or suppression of records, or in some cases perturbative methods may be employed.[235] But this can create another form of data non-use and produce bias in research findings, because individual records or items within the those records, where they occur in unique or low-copy numbers, may be amended or omitted to mitigate perceived risks of re-identification. Often, the more unusual records and extreme data items are the most interesting for research, since they may underlie pressing health problems. So this well-intentioned practice can limit external validity, as the application of results will gravitate to treating the mean characteristics and phenotypes in the population. Furthermore, the conditions for the use of anonymised data often preclude reversal of the process to lead back to individuals to highlight a worrying indicator in their data, since this would require permission

[231] 'The Secure Anonymised Information Linkage Databank' (2014) <http://www.saildatabank.com/> accessed 18 June 2014; Kerina H Jones et al, 'A case study of the Secure Anonymous Information Linkage (SAIL) Gateway: a privacy protecting remote access system for health related research and evaluation' (2014) Journal of Biomedical Informatics: special issue on medical data privacy.
[232] University of Western Australia, 'Prof D'arcy Holman' <https://www.socrates.uwa.edu.au/Staff/StaffProfile.aspx?Person=D%27ArcyHolman&tab=publications> accessed 18 June 2014.
[233] ICO, 'Key definitions of the Data Protection Act' <http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions#personal-data> accessed 18 June 2014.
[234] Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization'.
[235] ICO, 'Anonymisation Code of Practice'.

to hold identifiable information. So although the use of de-identified data is proving to be invaluable in data linkage research, it is still subject to forms of data non-use.

Governance frameworks are not static, and new legislation and regulations being introduced can have consequences for data use. At the same time as great efforts are being made to streamline and simplify governance procedures and to encourage greater data accessibility, other moves pose a serious threat to current research practice. This is most evident in the spectre of the proposed Data Protection Regulation (pDPR). Concerns have been widely expressed that this legislation could prohibit much medical and other epidemiological research due to amendments proposed by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE committee).[236] Among the most significant of these amendments is the removal of the research exemption, which (under section 33 of the current UK DPA[17]) provides certain exemptions for data processing activities for research and statistics, including in medicine and health.[237] In future, such processing would only be permitted with explicit consent of the data subject unless an exemption was sought for research of exceptionally high public interest. Another is the tightening of the definition of personal data and the regulation of pseudonymised data, defined as 'personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution' (Article 4(2a)).[238] This could impose disproportionate regulatory burden and undermine sophisticated data linkage and sharing infrastructures, such as Safe Havens. The European Parliament's position includes the amendments, but at the time of writing there is still a way to go before the final text is agreed. Numerous parties are contributing to sterling work co-ordinated by the Wellcome Trust to publicise and lobby for the interests of research for public benefit.[239] If the pDPR is passed as it currently stands, it will herald a new era of data non-use by creating insurmountable obstacles to research to the detriment of health and well-being.[240]

9.A.8.F Conclusions on non-use

The systematic searches used in this review uncovered little/no proven instances of harm due to the non-use of data, wherever they were conducted. By exploring some of the reasons for the non-use of data, with examples to demonstrate the principles, this section points towards a

[236] Corrette Ploem 'Proposed EU data protection regulation is a threat to medical research' (*BMJ News,* 2013) <http://www.bmj.com/content/346/bmj.f3534> accessed 18 June 2014.
[237] However, it is para 8, Sch 3 of the DPA, that if satisfied, provides a lawful basis for processing sensitive personal data for medical purposes (including medical research). Importantly, a Sch 2 condition would still also need to be met.
[238] pDPR, Article 4(2a) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN> accessed 29 June 2014.
[239] Wellcome Trust, 'Protecting health and scientific research in the Data Protection Regulation' (2014) <http://www.wellcome.ac.uk/stellent/groups/corporatesite/@policy_communications/documents/web_document/WTP055584.pdf> accessed 18 June 2014.
[240] The most-current, agreed upon text of the pDPR may be consulted here: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN.

better understanding of why the non-use of data is poorly recorded. One of the major issues is missing or non-available data, so that data are not present to be used or not in a format that can be used. Negligence rather than data non-use is likely to be cited in any legal case or report arising from harm, since non-use of data may be insubstantial, and it may be even more tenuous to attempt to prove it being the cause of an ill effect. Another issue is publication bias whereby undesirable results are not put forward and/or not accepted by journals. This is an important form of data non-use, but by definition it will be difficult to find. Governance frameworks, and their over-zealous administration, are often perceived as the greatest hindrance to research and data use in general. There is, of course, a duty to protect privacy, but there also needs to be a balance so that data are used safely for public benefit. Definitive instances of harm due to the non-use of data because of excess governance are unlikely to be found in searches, as they would be difficult to prove outright. More likely are delays in data use, or the preclusion of some studies altogether, so that the consequences are lost opportunities, and as such, are very real but more nebulous. The use of de-identified data is often a good solution to barriers posed by governance, but even so, it can also result in forms of data non-use, which are not easily uncovered. Thus, the problem of data non-use is much greater than it appears, and is arguably more dangerous to individuals and society than any privacy risks in sharing clinical data.[23] But its very nature, and the complex reasons why it occurs, make it difficult to ascertain and quantify with accuracy.

9.A.9 Conclusions on the implications for governance

Note: We consider now the implications for governance addressed thus far. We believe we have identified very important other considerations when we later examine disincentivisation.

The evidence raised important issues for the governance of health and biomedical data. The number one cause contributing to abuse of health and biomedical data was *maladministration*, which can also be understood as the epitome of poor governance practices. Thus the key implications for governance of health and biomedical data include the apparent need for *improvement over the effective monitoring of standards and procedures* that are *already in place* in the NHS and other healthcare organisations. This includes a need for *random spot checks* for compliance; *robust auditing procedures* for how data are accessed, transferred and generally used on and off premises; and *specific guidance* as to *particular uses of data* and especially for more sensitive data (e.g. faxes, emails, use of portable media etc.). Finally, the cases involving DNA profiles, raised important implications for the governance of health and biomedical data – namely, that *harm must be considered from outwith the narrow scope of actual harm* when planning and implementing good governance of health and biomedical data.

Finally, in *S and Marper*,[(EUC7)] involving DNA profiles, important implications were raised for the governance of health and biomedical data – namely, that *harm must be considered from outwith the narrow scope of actual harm* when planning and implementing good governance.

9.B Assessing the effectiveness of sanctions and remedies in light the prevalence of abuse uncovered

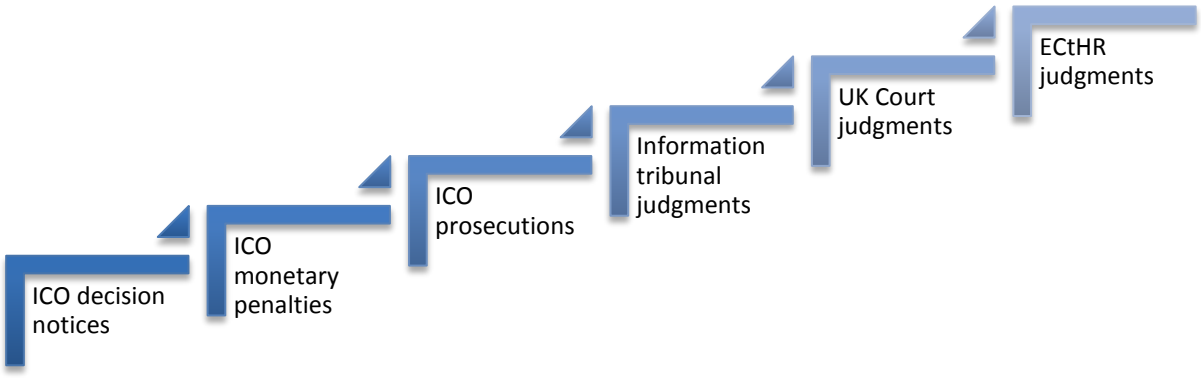
In light of the incidence of abuse uncovered, we now consider the relative effectiveness of sanctions and then remedies featured in the evidence. However, it is important to note, that the evidence may be limited by virtue of the potential use of gagging clauses, private investigations and confidentiality of proceedings. Sanctions will be considered on a scale from those serving the purpose of pre-empting greater abuses and those imposed after the fact, that is, after the abuse has occurred. Remedies will also be considered on a scale – from early interventions in a robust complaints procedure process to post-abuse remedies and compensation including awards of damage, but also forced cessation of processing data.

9.B.1 Sanctions

Several types of sanctions were found in the hard and soft evidence strands. Sanctions could be assessed from interventions at the pre-emptory stage where abuse has not occurred but where data handling has failed to meet legal standards or best practices. However, the evidence gathered brought forth only those sanctions imposed *post*-breach, when the abuse has already occurred (potentially, repeatedly). This is considered a logical result given that the evidence produced by this review would likely only focus on incidents of abuse, already subjected to sanctions, if publicly reported in the press or otherwise.

Figure 12 features the spectrum of sanctions specifically uncovered in the evidence, with an overview of those sanctions which no doubt were imposed but were not identified in the review.

Figure 12: Spectrum of sanctions uncovered in the evidence review



The sanctions *not* identified in the evidence review specifically include those that would be imposed at a pre-emptory stage, for example, as a response to an organisation's internal or ICO complaints procedures process, and thus would *not* be publicised (or thus uncovered in the evidence search). The role of these pre-emptory sanctions will be considered below whilst focusing simultaneously on the specific sanctions identified in order of the spectrum above.

9.B.1.A ICO Sanctions

The ICO plays an important role in auditing and ensuring the compliance of data controllers. Given its role in pre-empting further legal action in the courts, the ICO features first in the spectrum of sanctions. Although its enforcement remit includes the power to issue numerous sanctions *prior* the occurrence of serious abuse and thus more escalated actions including monetary penalties and prosecutions, none of the more pre-emptory enforcement actions detailed below involved health or biomedical data and/or were simply not published by the ICO. The ICO's *pre-emptory* sanctions that were not identified in the evidence included:

- **Information notices** requiring data controllers to provide the ICO with specified information regarding their processing of personal and sensitive personal data by a certain time;
- **Undertakings** that reflect a data controller's commitment to start a specific course of action to improve their compliance with the DPA;
- **Enforcement notices** and **'stop now' orders** where a breach of the DPA occurred and whereby the ICO requires data controllers to take or refrain from taking specific action, in order to bring themselves into compliance with the law;
- **Voluntary audits** by the ICO in consenting organisations, in order to spot-check compliance; and
- The service of **assessment notices** which notify a data controller that the ICO will conduct a compulsory audit to assess whether their processing of personal data follows good practice.[241]

The three ICO sanctions, which *were* identified in the evidence included:

- **Decision notices**, which represent 'the Information Commissioner's view on whether or not a public authority has complied with the Freedom of Information Act or the Environmental Information Regulations, following [an] investigation of a complaint. It can include legally binding steps for the public authority to follow.'[242]
- **Monetary penalties**, which are issued on the basis of serious contraventions of the DPA and if (a) the contravention was likely to cause substantial damage or substantial distress; and (b) was deliberate or (c) the data controller or person must or should have

[241] ICO, 'Taking action: data protection and privacy and electronic communications' <http://ico.org.uk/what_we_cover/taking_action/dp_pecr> accessed 29 April 2014.
[242] ICO, 'Enforcement Notices' <http://ico.org.uk/enforcement/decision_notices> accessed 29 April 2014.

known about the nature of the risk for such harm and failed to take reasonable steps to prevent it.[243]

- **Prosecutions**, where the ICO takes to court data controllers and individuals who have committed criminal offences under the DPA.

Decision notices issued by the ICO have the least implications for governance. Unlike the other sanctions featured, decision notices in the UK are specific to violations of the Freedom of Information Act and thus specific to *public authorities* only. More relevant to the scope and purpose of this report are the imposition of monetary penalties and the publication of these penalties by the ICO.

Importantly, '[u]ntil 2010, one of the biggest flaws of the [DPA] was arguably the limited range of offences under it, and a corresponding lack of power granted to the Crown (and, in England and Wales, to the Information Commissioner and Director of Public Prosecution) to enforce the Act.'[244] With the power to introduce monetary penalties for serious contraventions of the DPA, the ICO gained an important sanction that would promote compliance with DPA, serving as a disincentive to non-compliance with the Act – for both financial and reputational reasons. [245] The power to impose fines of up to £500,000 is significant enough to disincentivise serious breaches of the DPA, especially given the publication of these penalties that ensures bad press for offending data controllers. It is considered that monetary penalties serve an extremely important deterrent role in combatting the abuse of health and biomedical data, especially given the large proportion of monetary penalties served to NHS and other health care service bodies.

It is considered that monetary penalties serve an extremely important deterrent role in combating the abuse of health and biomedical data, especially given the large proportion of monetary penalties served to NHS and other health care service bodies. However, considering the purpose of the NHS, that is, to provide patient care, one should also be aware of the implications of harsh monetary penalties. For example, when Brighton and Sussex University Hospitals NHS Trust failed to decommission hard drives and these were placed for auction on eBay by a sub-contractor, the ICO imposed a record fine of £325,000.(News18) As the Trust's CEO commented, 'In a time of austerity ... we simply cannot afford to pay a £325,000 fine. ... [The amount would pay for] the delivery of 300 babies, 50 hip operations, 30 heart bypasses and 360 chemotherapy treatments'.(In26)

Finally, it is considered that the criminal prosecutions undertaken by the ICO serve a similar deterrent role in disincentivising criminal breaches of the DPA and thus promoting compliance. Furthermore and as related to social (rather than legal) conceptions of harm discussed in

[243] 'Data Protection Act 1998: Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998' 4.
[244] Gillian Black, 'Data Protection Reissue' in the *Stair Memorial Encylopaedia*, para 318.
[245] DPA, s 55A (added by the Criminal Justice and Immigration Act 2008 (c 4), s 144(1)).

Section 3.C *Harm in other contexts*, the ability for the ICO to undertake criminal prosecutions for criminal offences under the Act is particularly important to protect vulnerable segments of society. This ability helps to ensure that individuals who suffer harm as a result of such abuses but are without the wherewithal to pursue the case formally, are protected and/or compensated for the crimes committed against them.

9.B.1.B First-tier Tribunal (Information Rights) Judgments

Very much related to ICO sanctions are the judgments of the First-tier Tribunal (Information Rights). The Tribunal deals specifically with appeals from the ICO's issuance of enforcement notices, decision notices and information notices.[246] Given the single incident identified in the evidence reviewed of Tribunal proceedings, it suffices to state that the Tribunal's role in sanctioning contraventions of the DPA serves as an endorsement or rejection of the ICO's more pre-emptory sanctions and enforcement powers. Thus the role of the Tribunal, whilst 'higher' up in the spectrum of sanctions, is relatively less important to disincentivising the abuse of health and biomedical data. However, this is not to underestimate the importance of a 'final stamp of approval' from the judicial system, for 'softer' or more pre-emptory sanctions undertaken by the ICO. A stamp of approval can send important signals to data controllers that breaches of the DPA *will* be taken seriously.

9.B.1.C UK Court Judgments

Given that the spectrum of sanctions in Figure 12 generally follows a given abuse from the early complaints stage to the more escalated judicial pursuit of the incident, the role for UK Courts in sanctioning abuse of health and biomedical data is important in providing a further disincentive for poor data handling practices and harmful behaviour. The lack of case law dealing specifically with abuses of health or biomedical data as the abuse relates to either a breach of the DPA or other common law, first reflects the small percentage of claims that actually do go to trial. (See Section 1.D.2.) Secondly, this reflects the fact that many claims will be resolved long before reaching the more escalated stage of trial. The way complaints are resolved either by a particular organisation or the ICO is not available publicly or thus accounted for in the evidence. However, given the ICO's statement that they deal with tens of thousands of complaints every year and that only a fraction of that are reported as being subject to the sanctions identified above, would indicate the small fraction of abuse that ends up in front of UK Courts.

With these caveats in mind, the UK Court plays an important role in ensuring that the use of health or biomedical data complies not only with the specific (and narrow) provisions in the DPA, but also with more general principles at common law (i.e. breach of confidence or misuse of private information). This is in keeping with individuals' human rights (per the European Convention on Human Rights and in particular Article 8, which guarantees an

[246] ICO, 'Taking action: data protection and privacy and electronic communications'.

individual's right to private and family life, his or her home and his or her correspondence, against the interference by public authorities/governments). This serves an important sanctions role, and it overlaps with the ECtHR judgments considered immediately below.

9.B.1.D European Court Judgments

The European aspect of this review uncovered evidence of abuse adjudicated by the ECtHR. ECtHR judgments are situated as the final step on the sanctions spectrum (see Figure 12) and directly reflect the role the ECtHR within the judicial system of EU member states. The ECtHR intervenes only if it is alleged that a member state has failed to meet their obligations under the European Convention of Human Rights. The subject of this evidence review implicates the Article 8 rights of individuals (right to private and family life). Thus within the context of this report, the evidence features the ECtHR as a final venue for recourse to individuals where the ICO and/or UK Courts may have failed to uphold their rights in regards to their health or biomedical data. The evidence identified from the ECtHR offered insight into the more egregious cases of abuse of health or biomedical data, and largely from a European perspective – only four out of the fourteen cases identified were against the UK.(EUC2, EUC3, EUC7, EUC8) Most importantly, the ECtHR is considered to play an important role in the sanctioning of abuses that may go overlooked in any member state, and in making important contributions to understanding the (broader) scope of protection offered by Article 8 of the ECHR for health and biomedical data.[247]

9.B.2 Overall effectiveness of sanctions for abuse of health or biomedical data

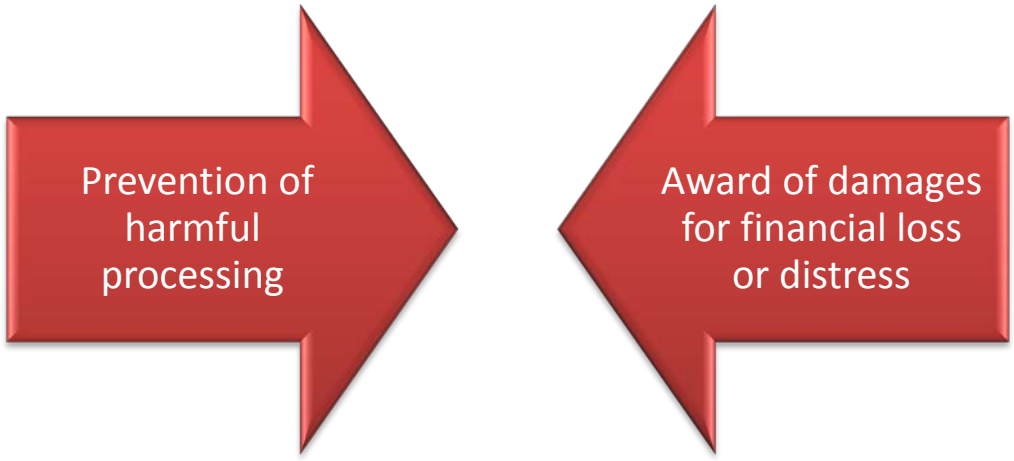
The evidence identified shows a narrow range of sanctions available when health or biomedical data have been abused. It is considered that the sanctions applicable to the abuse of health or biomedical data in the UK are not entirely ineffective, but also not fully capable of offering robust disincentives for further abuse. Because the 'softer' or more pre-emptory sanctions imposed at the earlier stage of the complaints process are not publicised, it was not possible to assess the effectiveness of a potentially wide portion of 'sanctions' available. However, the effectiveness of sanctions imposed at *later* stages (usually post-abuse) are limited in the UK to the narrow confines of the DPA (for the ICO), and slightly less so for UK Courts that may take a broader perspective in line with common law and human rights. In this regard, the ECtHR serves an extremely important role in providing sanctions for abuses that would otherwise be overlooked within the UK. In the next section, we consider the effectiveness of the remedies offered by these various sanctioning bodies – the ICO, Information Tribunal, UK Courts and ECtHR.

[247] For example consider the case of *S and Marper* (considered in depth in Section 9.A.7) the ECtHR was able to consider the issue of indefinite retention of DNA profiles and samples outwith the narrow confines provided for under UK law. This judgment made an important contribution to the understanding of privacy issues surrounding genetic data, and the capacity for human rights law to protect against disproportionate interferences with such rights under Article 8 of the ECHR.

9.C Remedies

As shown in Figure 13, the remedies identified in the evidence review were limited to two main types.

Figure 13: Remedies identified in the evidence review



This is considered as a direct consequence from the way compensation and non-compensatory remedies are framed in the DPA (detailed in Section 3.B). The DPA also provides a limited number of rights of actions for individuals for particular breaches of the Act. These are *not* considered remedies in the legal sense, given that remedies affect how rights are *enforced* and *satisfied* rather than the right in and of itself:

- The right of an individual to request access to the personal data held on them.[248]
- The right of an individual to request a notice from the data controller (in writing) that no decision taken was based solely on evaluation produced by automatic processing.[249]

Our assessment of the limited scope of remedies available under the law are affected by our broader understanding and more holistic conception of harm (detailed in Section 3.C) as encompassing not only legal conceptions but the social realities of harm. Given that the abuse of data can result in multiple types of harm (financial, legal, physical, social and psychological), the prevention/cessation of harmful processing and/or award of damages can only address a small aspect of harm caused to individuals. To further consider are "invisible harms" which arguably are neither addressed by current or proposed regulation of data.[250]

One notion of invisible harm was taken from the legal perspective, whereby invisible harms refer to a cause and effect from current trajectories in the era of big data. Here personal data

[248] DPA, s 7.
[249] DPA, s 12(1).
[250] Judith Rauhofer, 'Round and Round the Garden? Big Data, Small Government and the Balance of Power in the Information Age' (2014) 2014 University of Edinburgh, School of Law Research Paper Series, Research Paper Series 1-12.

are disclosed and inevitably shared with further public or private entities, often without individual consent or conscious knowledge.[251] The effect (and harm) is perpetuated by the improbability 'for individuals to appreciate, at the time of collection, how long their data will be stored, how it will be used in the future, for what purposes and by whom.'[252] Thus individuals' ability to make informed decisions or thus take relevant precautions against potential abuses of their data is extremely restricted.[253] Such invisible harms are not quantifiable in a way that would be recognised under current laws, and the single case where a court specifically found *no harm*(UKC14) underscores this notion of invisibility. Even cases of more 'visible' harms, especially those impacting broader public interests, are similarly unaccounted for under the law, whilst at the same time providing for protection of broader public interests as a means of justifying *use* of data[254] – there is little to be done where such uses impact or harm those interests negatively.

The prevention or cessation of harmful processing[255] can partially address the social and psychological impact, depending on how pervasive and widespread the data use was. However, restorative justice, which seeks to recuperate the psychological damage caused in events of harm, cannot be effectuated with eventual prevention of processing that will necessarily be subject to the delays associated with court procedure. This is even more apparent with the award of financial compensation for damages or distress arising out contravention of the DPA. The financial and psychosocial costs associated with pursuing a case to the point where compensation may or may not be awarded simply are not provided for in the often-nominal damages awarded.[256]

The evidence suggests that cases escalated to the level of the ECtHR will generally be awarded more 'generous' damages. However, this is limited to the particularly egregious and wilful breaches of human rights law (not the DPA). Furthermore, these cases are subject to an even longer procedure such that any award of damages will be unable to fully compensate for the loss of time spent on pursuing the case and/or address the psychosocial harms caused long before the ECtHR reviews the case.

[251] Rauhofer, 'Round and Round the Garden? Big Data, Small Government and the Balance of Power in the Information Age' 9.
[252] Rauhofer, 'Round and Round the Garden? Big Data, Small Government and the Balance of Power in the Information Age' 9.
[253] Rauhofer, 'Round and Round the Garden? Big Data, Small Government and the Balance of Power in the Information Age' 9.
[254] For instance, Sch 2 para 5(d) of the DPA provides that the processing of personal data will be lawful if necessary 'for the exercise of any other functions of a public nature exercised in the public interest by any person.' Here broader public interests are protected where using personal data will do so.
[255] Such as provided under s 10 (prevention) and s 14 (cessation) of the DPA.
[256] For example, *Douglas v Hello!*, the Court only awarded nominal damages (£50 each). [2003] EWHC 786 (Ch) para [289].

9.C.1 Overall effectiveness of remedies for abuse of health or biomedical data

In sum, the overall effectiveness of remedies for harm, caused by abuses of health or biomedical data, are considered *ineffective* given the broader understanding of harm provided for in this report. Remedies are limited to those that can be sufficiently supported by the required criteria under the law and do *not* reflect the totality of harmful effects that can be caused either to individuals or to indeed broader public interests.

9.D Addressing incentives and disincentives to abuse

Whilst the good governance of health and biomedical data, supported by effective sanctions and remedies for individuals harmed, can do much to address the prevalence of abuse uncovered in this review, there remains strong incentives to abuse data. Aside from the *causes* for abuse identified within the evidence (e.g. maladministration, human error) we consider briefly the further incentive perpetuated by the black market for data. Within this context, the prevalence of sophisticated re-identification attacks will also be considered.

9.D.1 The black market for data

Alongside the issues raised by poor governance, the existence and growth of the black market for data further incentivizes and facilitates abuse of health and biomedical data. A wealth of independent research on the black market for data has been undertaken predominantly in the US and may be indicative of the increased scale and sophistication of the black market there. This may be supported by the difference in reported incidents of *theft* of health or biomedical data report in the Twitter evidence – featuring only one case in the UK (TW45) out of twenty identified incidents (eighteen in the US, one in Zambia). Thus, the research discussed below may be representative only of the black market in the US, particularly where identity theft can bring real income against the backdrop of medical insurance. Although citizens in the UK enjoy free medical care, the US trends could have potential implications for the UK in future.[257]

As indicated in the RAND Corporation's exhaustive report on cybercrime, it is apparent that the growth of black markets where unlawfully obtained sensitive data are sold is without doubt growing in scale and sophistication.[258] What once comprised scattered individuals seeking monetary gain and/or notoriety are now 'financially driven, highly organised and sophisticated', representing groups that tend their unlawfully obtained wares in virtual marketplace using digital currencies such as Bitcoin, Pecunix, AlertPay, PPcoin, Litecoin and Feathercoin.[259] The black market for data takes place on difficult to track darknets, virtual private networks and on

[257] Or presently; the lack of evidence of theft of data in the UK does *not* (in the slightest) mean this is not occurring.
[258] Lillian Ablon, Martin Libicki and Andrea Golay 'Markets for cybercrime tools and stolen data: Hackers' Bazaar' (Rand Corporation 2014) <http://www.rand.org/pubs/research_reports/RR610.html> accessed 29 April 2014.
[259] Lillian Ablon, Martin Libicki and Andrea Golay 'Markets for cybercrime tools and stolen data: Hackers' Bazaar'.

the deepweb.[260] In the black market of data, the 'goods' and services can include *Enabling Services* that help identify targets (the data and organisations holding the data), *Initial Access Tools* to infiltrate the target's system and thus bring the perpetrator to the target's *Digital Assets* (assets in this context include personal and sensitive personal data). Thus, the cycle of obtaining data illegally is complete.[261]

Services offered on the black market can operate as a one-stop-shop to service the full lifecycle of a data breach. Increasingly, disparate sets of data on an individual are being combined to form 'kitz'.[262] Also available are 'fullz', which are electronic packages containing personal data including, for example, health insurance numbers.[263] Kitz range from USD$1,200 – 1,300, whilst fullz containing verified health insurance credentials, may cost up to an additional USD$500. However, others estimate the approximate cost of a medical record at USD$20.[264]

Also from the US, the Ponemon Institute estimated that, in 2013, 94% of medical institutions were been attacked.[265] More recently, a US-based study that gathered data on malicious traffic by using the honeypot technique reported 72% of malicious traffic recorded as targeting health care providers.[266] Further taken from the US experience, 90% of healthcare organizations believe that breaches are harmful to patients, and resolving medical identity theft causes victims a financial loss.[267] Indeed, the main motivation for attacks on the healthcare industry is financial.[268] Outside of financial gain, personal health information can

[260] Darknets are 'anonymising private networks using encryption and proxies to mask identities e.g. Tor, I2P', whereas the deepweb refers to 'web content that is not indexed by search engines such as Google but that is accessible through conventional means'. Lillian Ablon, Martin Libicki and Andrea Golay 'Markets for cybercrime tools and stolen data: Hackers' Bazaar' 66.

[261] Lillian Ablon, Martin Libicki and Andrea Golay 'Markets for cybercrime tools and stolen data: Hackers' Bazaar' 10.

[262] Robert Lemos 'Cyber-criminals selling fraudulent identity 'kitz' on the web black market' (*Eweek*, 17 July 2013) <http://www.eweek.com/security/cyber-criminals-selling-fraudulent-identity-kitz-on-web-black-market/> accessed 29 April 2014.

[263] Elizabeth Clarke, 'Hackers sell health insurance credentials, bank accounts, SSNs and counterfeit documents, for over $1,000 per dossier' (*Dell Secureworks blog*, 15 July 2013) <http://www.secureworks.com/resources/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents/> accessed 29 April 2014.

[264] Jenny Mangelsdorf, 'New healthcare'. New risks: Intermountain's healthcare cybersecurity challenge' (*CSC World Magazine*, 2013) <http://www.csc.com/health_services/publications/91654/99357-intermountain_healthcare_s_cybersecurity_challenge> accessed 28 April 2014.

[265] Ponemon Institute, '2013 Survey on medical identity theft' (*Ponemon Institute*, 2013) <http://medidfraud.org/2013-survey-on-medical-identity-theft/> accessed 29 April 2014.

[266] Barbara Filkins, 'Health care cyberthreat report: Widespread compromises detected, compliance nightmare on horizon' (*SANS Institute/Norse Corp*, 2014) <http://norse-corp.com/HealthcareReport2014.html> accessed 29 April 2014.

[267] Bob Krenek, 'Five differentiating factors of a healthcare breach' (*Experian* 10 April 2012) <http://www.experian.com/blogs/data-breach/2012/04/10/5-differentiating-factors-of-a-healthcare-breach/> accessed 29 April 2014.

[268] Gal Landesman, 'Cyber threats to the healthcare industry' (*SenseCy*, 17 February 2014) <http://blog.sensecy.com/2014/02/17/cyber-threats-to-the-healthcare-industry/> accessed 29 April 2014.

also be sold on the black market so that others may access health care or bill insurance companies for alleged health care. [269]

This begs the question, to what degree can US-based incidence rates be extrapolated to the UK? Due to the NHS ethos of free care for all, non-financial motivations for medical identity theft are probably less likely in the UK, reflecting the *low* incidence of theft uncovered in the *hard* evidence; versus high incidence of theft uncovered in the Twitter evidence and in the Twitter evidence only. However, the value of health data in and of itself on the black market likely remains on par with the value attributed to such data in the US – given its potential for targeted marketing, scams etc.

It is useful to consider at this point another trajectory of cyber attacks in the healthcare setting: the targeted attacks of medical devices for which the incentives can only be assumed – a desire to cause physical harm to the subject. This concern was acknowledged by the US Food and Drug Administration that has issued guidelines for the technical security of medical devices.[270] In such attacks, medical devices can be 'infected' with malware, causing the equipment to be slowed down and thus not work properly. This has been the case regarding foetal monitors in intensive care wards,[271] with further vulnerabilities exposed in wireless implanted defibrillators.[272]

There is no consensus as to whether we will see an increase in cyber attacks in the UK, nor at which rate the black market will grow. However the key projections and predictions for the black market,[273] its targets and actors are:

1	Darknet activities will increase	Actors likely to be better vetted and enjoy greater anonymity; increasing payments in cryptocurrencies poses fewer risks (e.g. those associated with money laundering).
2	'Ability to attack will likely outpace the ability to defend' (p.31)	Attacker needs to know only one method of attack; defender needs to know all methods of attack.
3	Attackers methods and tools will become more innovative	As security and law enforcement develops, so will attackers' encryption, vetting and operational security.
4	Targets will increase	Alongside the increase in digital data, hyperconnectivity, social media and mobile devices.
5	Crime, vulnerability and human error	Cybercrime will increase; vulnerability will continue; human error will remain a point of weakness.

[269] Dan Tynan, 'The next data theft target: Your medical records' (*Yahoo! Tech.*, 18 February 2014) <https://www.yahoo.com/tech/the-next-data-theft-target-your-medical-records-77113382628.html> accessed 29 April 2014.
[270] 'Medical device security alert notice' (US Food and Drug Administration, 13 June 2013) <http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm> accessed 28 April 2014.
[271] Gal Landesman, 'Cyber threats to the healthcare industry'.
[272] GAO (US Government Accountability Office), 'Medical devices: FDA should expand its consideration of information security for certain types of devices: Report to congressional requesters' (31 August 2012) <http://www.gao.gov/products/GAO-12-816> accessed 29 April 2014.
[273] Lillian Ablon, Martin Libicki and Andrea Golay 'Markets for cybercrime tools and stolen data: Hackers' Bazaar'.

6	Attacker profile	Outsourcing (operators for hire, brokers) will increase; digital-savvy generation will take over the market; best skilled hackers likely to move to grey market; lower skilled hackers will take over the black market.

9.D.2 Re-identification attacks

Relatedly, the phenomenon of re-identification attacks warrants discussion in the context of potential motivations to abuse health and biomedical data. Although evidence of re-identification attacks did not feature in the UK evidence, the thefts and technical security breaches that *were* identified were indicative of a growing sophistication of targeted attacks of databases with large amounts of sensitive health or biomedical data. Furthermore, the *motivations* behind re-identification attacks vary significantly from the other abuses identified in this evidence review and require distinction.

For instance, the theft of health or biomedical data may be motivated by financial gain. Motivations for abuse can also take more benign forms, where health data are accessed purely to satisfy the curiosity of an individual. In the case of re-identification attacks, the motivation may be the adversary's identification of a particular individual's record when they know that individual is included in a particular database,[274] or the goal may simply be to re-identify as many records as possible[275] in order to expose the weaknesses of an organisation's technical security and/or to broadcast the adversary's technical prowess.

Of the evidence reviewed, we found nothing to indicate that re-identification attacks, however, recent work on the re-identification of genomic data, perceived to be 'anonymous', has raised concerns.[276] Gymrek's et al 2013 work on re-identification of genomic data demonstrated that 'full identities of personal genomes can be exposed via surname inference from recreational genetic genealogy databases followed by Internet searches.'[277] Specifically, the study showed that the combination of a surname with other types of metadata, including age and state, can be used re-identify an individual's personal genome.[278] In response to this, key research funders in the UK have issued guidance and importantly recommended sanctions for researchers that attempt to re-identify anonymised data sets.[279] Given the different motivations for re-identification attacks, it is important that stakeholders involved in facilitating access to

[274] El Emam, *Guide to the De-Identification of Personal Health Information* 169.
[275] El Emam, *Guide to the De-Identification of Personal Health Information* 169.
[276] Here we reference El Emam's work on de-identification which lists eight of the most well known re-identifications attack, most of which occurred in the US (one in Canada).
[277] Melissa Gymrek et al, 'Identifying Personal Genomes by Surname Inference' (2013) 339 Science 321–324, 321.
[278] Melissa Gymrek et al, 'Identifying Personal Genomes by Surname Inference'.
[279] Cancer Research UK, the Economic and Social Research Council, the Medical Research Council and the Wellcome Trust issued a joint statement in response to guidelines issued by the Expert Advisory Group on Data Access (EAGDA). Their statement agreed with the EAGDA's approach to deliberate attempts to re-identify individuals in anonymised data sets – that such action should be considered 'malpractice' and met with appropriate sanctions. The Wellcome Trust, 'Research funders outline steps to prevent re-identification of anonymised study participants', (24 March 2014) <http://www.wellcome.ac.uk/News/Media-office/Press-releases/2014/WTP055974.htm> accessed 29 April 2014.

data, ensure appropriate – and the harshest of – sanctions are in place for deliberate attempts to re-identify otherwise anonymous health or biomedical data. This will at least serve as a disincentive to those *within* the health and biomedical sector (but not third party adversaries).

9.D.3 Disincentives

The Sections 9.D.1 and 9.D.2 address malicious attacks motivated by, in Kilger et al's words, MEECES: money, entertainment, ego, cause (that is, ideology, aka hacktivism), entrance to social groups and status.[280] The focus in this sub-section shifts to possibilities for disincentivisation to abuse. Normally understood as a financial disadvantage, we explore here an alternative – raising awareness of the data handler, appealing to and/or modifying personal/professional values and standards and bringing about behavioural change.

Before doing so, it should be acknowledged that doctors and other health-care professional are often faced with data protection decisions that involve data protection and record-keeping during patient treatment, or may have to answer for their decisions post-treatment. The members only Medical Defence Union (MDU) has a medico-legal team available to give advice on specific cases. However, its Annual Reports provide useful case studies of, amongst other things, correct data handling and the importance of correct record keeping, listed in the Reports' sections 'Cautionary Tales'. These reports (covering also the MDU's specialist dental division, the DDU) are in the public domain and available to download.[281]

As we noted under 9.B.2 (page 140), applicable sanctions in the UK are not entirely ineffective, but also not capable of offering rigorous disincentives to rule out further abuse. In addition, some sanctions in place serve to act as a deterrent for the data controller and his or her organisation. For the data handler, disciplinary hearings, dismissals, being struck off and potential prosecution are formal paths to disincentivisation. Against the backdrop of the MEECES motives, successful abuse can promote feelings of self-worth. For data handlers in this category, getting caught is likely a known potential risk. In other words, the deterrent is ineffective.

9.D.3.A The repeat offender

Some individuals are repeat offenders, and we can only speculate why this might be. We offer here just two of the many sound propositions offered by psychology.[282] Firstly and looking at

[280] Max Kilger, Ofir Arkin and Jeff Stutzman, 'Profiling' in *The honeynet project. Know your enemy: learning about security threats* (2nd edn, Addison Wesley 2004) 509-510 <http://old.honeynet.org/book/Chp16.pdf> accessed 24 June 2014.

[281] Medical Defence Union Limited, 'Report and Accounts 2011 including cautionary tales' (2012) 14-33 <http://www.themdu.com/~/media/Files/MDU/Publications/Annual%20reports/2011%20annual%20report%20and%20accounts.pdf> accessed 29 June 2014; Medical Defence Union Limited, 'Guide. Support. Defend. Including cautionary tales' (2013) 15-33 <http://www.themdu.com/~/media/Files/MDU/Publications/Annual reports/2012 annual report and accounts.pdf> accessed 20 June 2014.

[282] There is, for example, a wealth of research on risk-taking behaviour. It goes beyond the remit of this report to discuss antecedents of such behaviour.

personality traits, an individual who scores low on the agreeableness scale is motivated more by self-interest than by wanting to get along with others, is less kind and generally has little concern for the well-being of others.[283] Secondly we turn to Kohlenberg's Theory of Moral Development. [284] According to Kohlenberg, there are six stages of moral development over the life-course, whereby only 10-15% of adults reach stages 5 and 6. Only those who reach stage 6 (post-conventional morality) are likely to uphold universal principles in the knowledge that these apply to all individuals. Those who do not may not have internalised the wider rules of society: upholding the law is not seen as a necessity. The chances of a re-education programme being successful are very low.

9.D.3.B Other 'offenders'

Before discussing those offenders who *can* modify their behaviour, it is essential to consider the following hypothetical questions.

> **Which abuse is more severe? An act where thousands of encrypted patient records are lost and no harm/impact known? An act where a few named patients' details are lost and one patient has been harmed/felt a negative impact?**

We will return to these questions later.

Coming back to other offenders, it is important to distinguish between those who have acted with intent (but who have the ability to learn from the experience) and those whose actions are unintentional. We consider firstly those who have acted with intent.

9.D.3.B.1 Staff who have acted with intent but who have the ability to learn from the experience

For some, getting caught after abusing or misusing data can bring feelings of shame at the psychological level, and lead to ostracism and exclusion on the social level. We argue that, where the offender acts with intent, legal and regulatory sanctions are in place that may be effective or – based too on psychological variables – ineffective. We need to turn to the actual incident(s) of abuse and, crucially, the motivation behind it or them.

Where the action was intentional, we propose that re-education is possible, but certainly not in all cases. Taking MEECES (see Section 9.D.3 *Disinenctives*) as starting point, there can be a unique set of personal and psychological circumstances specific to the offender. Two examples were given above in Sections 7.B.2.A.2 and 7.B3.C. In the first case, a nurse gave

[283] Robert R McCrae and Paul T Costa, *Personality in adulthood* (The Guildford Press 1990); *The NEO PI-R Professional Manual* (Guildford Press 1992); *Personality trait structure as a human universal* (1997) 52 American Psychologist 509-516.
[284] Lawrence Kohlberg, 'The Claim to Moral Adequacy of a Highest Stage of Moral Judgment' (1973) 70:18 Journal of Philosophy 630–646; 'The Philosophy of Moral Development' in *Essays on Moral Development* (Harper & Row 1981).

patients' details to her boyfriend working for a company handling personal injury claims.(news32) This was undisputedly the wrong thing to do. However, she was so distraught at her wrongdoing that she murdered her daughter and attempted to then go on to commit suicide. We can only speculate on why she offended to start, but the reaction of a planned extended suicide suggests that an unhealthy relationship to her partner and/or mental ill health was involved. In the second case, a radiologist accessed pregnant patients' records.(TW60) Her reason for this was that she had a drug addiction, had lost her baby because of it, and wanted to gather information from patients with a drug addiction, to see which services they had accessed. This too was undisputedly the wrong thing to do. However, it would seem like a case of desperation (distraught over death of baby? lack of trust in the 'relationship of confidentiality'?) when a health-care professional does not access formal services.

These are two quite exceptional cases. Nonetheless, it would be unrealistic to assume that the methods we suggest below would work equally well for all. For those who would continue to or be allowed to work in their area, there is an array of possibilities that could assist the offender in realising the (potential) impact of his or her action.

Non-confrontational discussions should be held at the workplace, in order to gauge as clearly as possible the real motives behind the abuse. Indeed, it is known that the culture of blame (or looking for a scapegoat) is cowardly at best, and importantly it not only fails to resolve a status quo, but also provides the seed for further development of an oppressive culture. The NHS across the UK is notorious for this.[285]

Whatever the underlying motivations, not protecting patients' (or fellow colleagues') privacy and upholding their dignity speaks against the values and moral standards of health-care professionals. It is these values that need to be re-addressed. In the process of seeking to modify behaviour, it is important to distinguish between **compliance** and **conformity**, two terms that are very similar but also very different.[286] Compliance is the more active form, where the individual can modify their behaviour based on explicit or implicit requests made by others, usually those in authority. This means that we would see behavioural change, but the values and moral standards mentioned above are not necessarily internalised, that is, the individual 'does the right thing because they have been told to'. Conformity on the other hand is a more passive phenomenon. Individuals who conform will adjust not only their (external)

[285] Matthew Limb, 'Need for accountability should not result in "toxic" blame culture in NHS, conference hears' (*BMJ News*, 21 March 2014) <http://www.bmj.com/content/348/bmj.g2282> accessed 29 June 2014; Yvonne Coghill 'Empowering and enabling cultures.' (*NHS Leadership Academy* 12 August 2013) <http://www.leadershipacademy.nhs.uk/blog/about/blog/empowering-and-enabling-cultures/> accessed 22 June 2014; People Opportunities Ltd, 'Exploring Bullying and Harassment in the CQC: Summary document' (*People Opportunities Ltd*, July 2013) <http://www.cqc.org.uk/sites/default/files/documents/bullying_and_harassment_in_cqc.pdf> accessed 22 June 2014.

[286] Robert B Cialdini and Noah J Goldstein, 'Social Influence: Compliance and Conformity' (2004) 55 Annual Review of Psychology 591-621; Tracy Levett-Jones and Judith Lathlean, 'Don't rock the boat': Nursing students' experiences of conformity and compliance' (2009) 29 Nursing Education Today 342-349.

behaviour, but also their (internal) attitudes and beliefs, that is, the individual 'does the right thing because they want to'.

One way of getting the message across, about the implications for the subject of data abuse, is through inducing empathy (facilitating emotional capacity), that is, engage the offender in a perspective-taking exercise (utilising the offender's cognitive skill).[287] A workshop with a qualified facilitator/tutor could assist the offender to understand the consequences of his or her actions (i.e. know how the subject might feel) and the real impact of his or her actions (i.e. feel with or for the subject). Such techniques are being employed increasingly, for example by bringing offenders fact to face with their victims.[288] In the context of data abuse, even if the subject were known to the offender, it would be logistically naïve and morally questionable to bring together them together.[289] However, consideration could be given to finding a method of communicating real-life messages about the impact to the subject, remembering that the goal is to bring about attitudinal change (and thus behavioural change).

9.D.3.B.2 Staff where abuse was unintentional

The reasons behind an unintentional abuse of data can vary. Hypothetically and for example, it could be due to an oversight or carelessness because of extreme workload pressures (e.g. front-line staff), or due to the member of staff not realising that the act did constitute abuse (e.g. inadequate staff training), or a host of other reasons. What differentiates this member of staff from the offender described above is that we can assume a willingness to conform to the values of protecting patients (and other colleagues) from breaches.

Different reasons for the abuse require different actions. As with the offender, a non-confrontational discussion should be held at the workplace, in order to gauge as clearly as possible why the abuse occurred. Crucially and particularly in cases such as these, blame is futile. Let us consider here another extreme case, that of Jacinta Saldanha, the nurse who completed suicide after disclosing information on the well being of the Duchess of Cambridge to two Australian radio DJs posing as the Queen and the Prince of Wales. Her employer, King Edward VII's hospital, described her as '*an excellent nurse and well-respected and popular with all of her colleagues*', and the CEO of the Royal College of Nurses found it '*deeply saddening that a simple human error due to a cruel hoax could lead to the death of a*

[287] C Daniel Baston, Shannon Early and Giovanni Salvarini, 'Perspective Taking: Imagining How Another Feels Versus Imaging How You Would Feel' (1997) 23:7 Personality and Social Psychology Bulletin 751-758; C Daniel Batson et al, 'Empathy, attitudes and action: Can feeling for a member of a stigmatized group motivate one to help the group' (2002) 28:12 Personality and Social Psychology Bulletin 1656-1666.

[288] An example is the Offender Behaviour Programme, accredited by the Ministry of Justice. See <http://www.justice.gov.uk/offenders/before-after-release/obp> accessed 29 June 2014.

[289] When considering the act itself, the fine distinction between front-line staff with patient contact and other staff (e.g. back-office staff) should be kept in mind. There are psychological differences between the offender-subject relationship. Is the subject known (with all the dynamics that that entails) or is the subject anonymous (with all the dynamics that that entails)?

dedicated and caring member of the nursing profession.'[290] In the same article, the hospital claimed it had '*been supporting [Jacinta] throughout this difficult time*.'

This case perhaps demonstrates the need to keep the goal of the discussion at the forefront. It should look to seek ways to support the member of staff in ensuring that such abuse does not occur again. Equally importantly, it should establish how much responsibility lies with the staff member, and how much with the employer. Both parties may need to take remedial action. Taking the two examples given at the start of this section, in the first (extreme workload pressures), simply reminding the member of staff of the need to ensure that data (particularly paper records) are kept safely and securely is probably unhelpful. Rather, the working environment and conditions[291],[292] might be the underlying cause of the abuse. In the second case, a refresher course on data security would be useful, but in a novel form.

9.D.3.C Data protection awareness (re-)training – bringing home the real-life message

Many would acknowledge that traditional staff courses on data protection issues are a) somewhat dry and b) very theoretical. They provide a sound knowledge base that data handlers need to have. At the same time, errors in procedures that result in harm/impact may have real-life consequences for the data subject. We believe that – as an alternative or together with formal 'teaching' – providing workshops and similar that highlight patients' stories can serve very well to bring the message home about just how devastating the impact of the abuse can be. In the context of improving the patient experience (that is, in the realm of clinical care) this approach comes highly recommended by the King's Fund as a response to the Francis Report,[293] and is regarded by the NHS as very effective.[294] Indeed, patient stories are already available in film form in the public domain.[295] Finally, a number of cases have been identified and discussed in the soft evidence of this report.

We also suggest that **this real-life approach in delivering education on data protection issues in the health care setting should form part of the material delivered to medical**

[290] 'Statement from the King Edward VII's Hospital on the death of nurse Jacintha Saldanha' (*The Telegraph*, 7 December 2012) <http://www.telegraph.co.uk/news/9730305/Statement-from-the-King-Edward-VIIs-Hospital-on-the-death-of-nurse-Jacintha-Saldanha.html> accessed 19 June 2014.
[291] A 2012 survey reported that children's social workers are working on average 9.5 extra hours per week. Johnathan Coxon, 'Social worker and overtime: what to do if you're heading towards burnout' (*Community Care*, 12 December 2012) <http://www.communitycare.co.uk/2012/12/12/social-workers-and-overtime-what-to-do-if-youre-heading-towards-burnout/> accessed 24 June 2014.
[292] In its 2013 survey, the Royal College of Nursing found that 56% of nurses work extra hours on every shift or several shifts a week. Royal College of Nursing, 'RCN employment survey 2013' (2013) <http://www.rcn.org.uk/__data/assets/pdf_file/0005/541292/Employment_Survey_2013_004_503_FINAL_100214.pdf> accessed 20 June 2014.
[293] The King's Fund 'Patient-centred leadership: Rediscovering our purpose' (The King's Fund, 2013) <http://www.kingsfund.org.uk/publications/patient-centred-leadership> accessed 26 June 2014.
[294] NHS Institute for Innovation and Improvement, 'Transforming patient experience: The essential guide'<http://www.institute.nhs.uk/patient_experience/guide/home_page.html> accessed 27 June 2014.
[295] Patientstories, 'Films' <http://www.patientstories.org.uk/films/> accessed 27 June 2014.

and nursing students, and to others training in this sector. Lectures are not enough. Tutorials/workshops with high student participation are key.

9.D.3.D Our cautionary tale

Earlier in this section we posed hypothetical questions, namely

> **Which abuse is more severe? An act where thousands of encrypted patient records are lost and no harm/impact known? An act where a few named patients' details are lost and one patient has been harmed/felt a negative impact?**

As we discussed under Sections 4.A, 4.B. and 4.C, ranking the severity of abuse is not as straightforward as one might presume. Based on the hypothetical questions above, to what degree does the number of those affected play a role? Has the abuse had an impact on any specific individual(s), and if so, to what degree? Was the abuse intentional or unintentional? If intentional, was the motivation wilful/malicious or benign (e.g. idle curiosity, accessing medical records of a significant other at their request) or somewhere in between (e.g. the newly qualified doctor accessing the case notes of patients' with particular illnesses/conditions of special interest to him or her)?

We consider three aspects here.

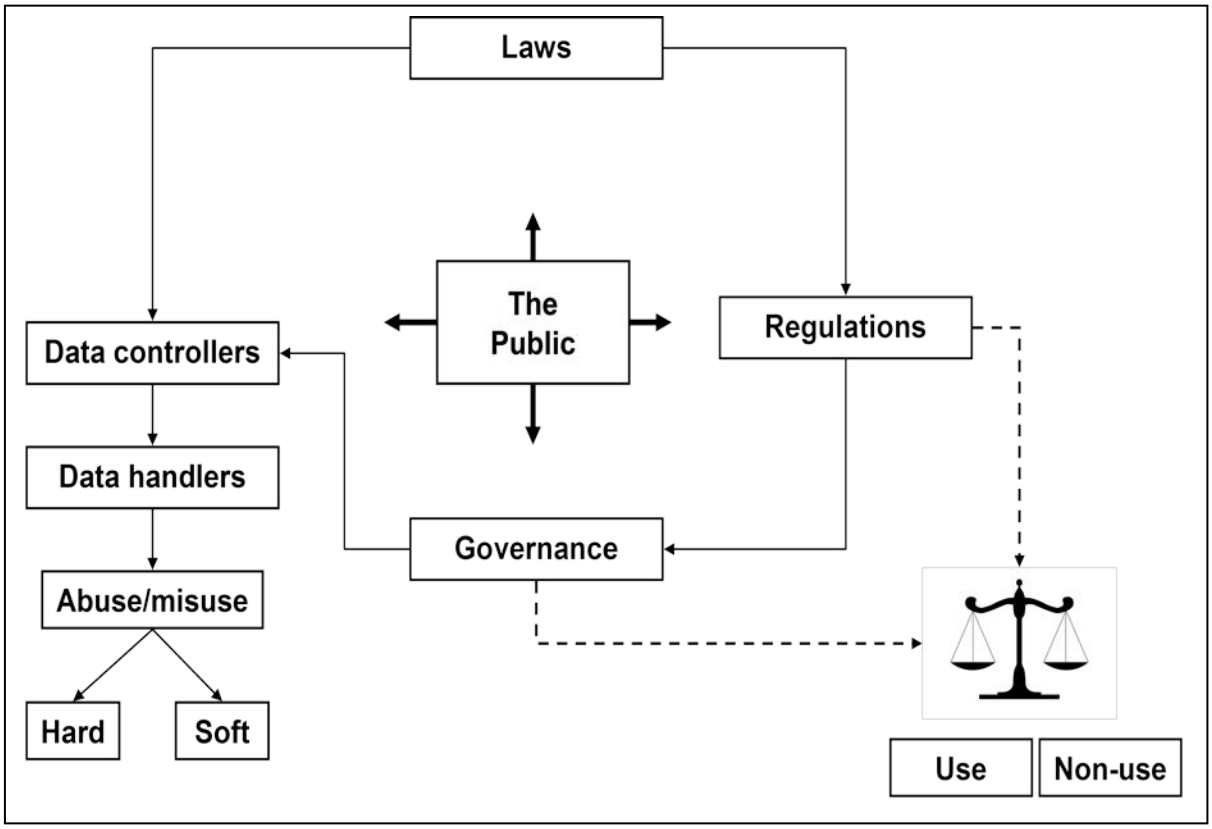
- The cost of non-use of data.
- The severity of penalty for a misdeed or wrongdoing should be reasonable and proportionate to the severity of the infraction ('let the punishment fitting the crime'). [296]

The degree to which we should consider the impact of severe penalties.

When considering these, we draw on the data protection landscape in the UK, and depict this in Figure 14 in a highly simplistic way. Essentially, the UK legal system dictates the landscape. Alongside European Union law with its directives, UK law serves to inform regulations. These in turn in part inform information governance. Data controllers are obliged to translate all of these into their policies and practices.

[296] Robert Nozick 'Philosophical explanations' (Harvard University Press 1981) 366–368.

Figure 14: The data protection landscape in the UK (simplified)



Thus far we have discussed in depth in this section the implications of our findings for governance and given a detailed account of the implications of the non-use of data. We return here to the implications of non-use of data, and suggest a balanced approach when under consideration by the regulators and by Governance Boards.

In the clinical research setting the GMC in its *Good Practice Research Guide* states that the researcher '*must make sure that foreseeable risks to participants are kept as low as possible … [and in addition … be satisfied] that the anticipated benefits to participants out weigh the foreseeable risks'*.[297] For medics, treating patients at their most vulnerable, namely at end of life, the GMC in its *Good Medical Practice: End of life care* stresses that all decisions must be in the patient's best interests. '*This means weighing the benefits, burdens and risks of treatment for the [here child]*'.[298] Further, *'[t]he benefits, burdens and risks associated with a treatment are not always limited to clinical considerations, and [the physician] should be careful to take account of the other factors relevant to the circumstances of each patient'*.[299]

[297] General Medical Council, 'Good practice in research: Good research design and practice' <http://www.gmc-uk.org/guidance/ethical_guidance/6003.asp> accessed 23 June 2014.
[298] General Medical Council, 'Neonates, children and young people' <http://www.gmc-uk.org/guidance/ethical_guidance/end_of_life_benefits_burdens_and_treatment_risks.asp> accessed 23 June 2014.
[299] General Medical Council, 'End of life care' <http://www.gmc-uk.org/guidance/ethical_guidance/end_of_life_benefits_burdens_and_risks.asp> accessed 23 June 2014.

Therefore the treating physician and the clinical researcher alike are empowered to make the ethically correct decisions regarding the weighing up of benefits against foreseeable risks, and in the case of the treating physician, to consider his or her decisions on a case-by-case basis. We do indeed put our lives in their hands. We suggest here that, when the benefits and risks of data linkage are not balanced, overly cautious decisions can result. When these decisions are imbalanced and against data linkage, a highly likely result is that medical advancements will be impeded, and the repercussions can affect whole patient groups and their significant others, placing a large financial and resources burden on both the NHS and Social Services in the future.

Secondly we turn to 'the punishment fitting the crime' and the impact of the punishment. As also depicted in Figure 14, the data controller oversees data handlers within an organisation. The data handlers can be front-line clinical staff, administrative staff, technical staff etc. who come with specific areas of expertise and varying levels of access to patient data. We have noted that, when data abuse occurs, there are clearly cases where disciplinary action through to dismissal is the only option (depicted in Figure 14 as "hard"). However, the goal should be to modify the behaviour (and hopefully also the attitude) of the offender, or in the case of unintentional abuse, raise awareness through seminars, workshops etc. Here we suggest a "soft" approach. The costs and implications of too harsh a punishment can be:

- The culture of blame and bullying in the NHS will continue to thrive.
- This brings with it fear, and the offender may be too traumatised to process any further training and thus be unable to modify his or her behaviour.
- Where a highly qualified member of staff is dismissed, those skills are then no longer available to serve the patient. Current patients may be let down, the expertise on the ward is lost, and already direly long waiting lists may grow even more.

If we do not consider this soft approach as a viable addition to disincentives and sanctions, there is a legitimate fear that the laws, rules and regulations governing the NHS will continue to grow, and most worryingly this to little effect. The NHS is overburdened to the point that patient care is suffering. And we must do all we can to prevent this situation deteriorating even more.

Not least, we end this section with 'the public', depicted centrally in Figure 14. The public are the beneficiaries of good medical research and healthcare. Simultaneously it is their data that are at risk of harm. Fortunately for us, we live in a democracy where terms such as citizenship, participation and empowerment are becoming increasingly higher on social and political agendas. The public can and should be involved in all aspects of civil life. We urge that we – 'the experts' – consult with them on such important aspects of our lives. In this respect, it is they who are 'the experts'. And as a final word of caution, consulting with the public should not be a tick-box exercise. We must listen to these very important stakeholders.

9.D.4 Conclusions on motivations

In considering selected motivations to abuse health or biomedical data, as informed by the evidence gathered, incentives ranged widely from financial motivations, to other forms of self-gain including a hacker demonstrating their technical prowess. In light of the range of incentives to abuse health or biomedical data, the importance and role for good governance in the first instance and effective sanctions when abuses do occur, become apparent. In the next section, we consider areas warranting further and future research, in light of the scope and limitations of this evidence review and in specific consideration of what evidence was *not* uncovered. We then conclude the report by reviewing the scope of the evidence review, the important distinctions made between the three stranded approach (hard, soft and Twitter), and finally the key conclusions that emerged from the evidence.

10. Future Research

The evidence review highlighted several areas where further and future research would be warranted outwith the scope and limitations of this report. We strongly recommend reducing the scope of any piece of future work, giving opportunity to explore in-depth and exhaustively. Here we provide indications of the topic and nature of potential areas of interest for both NCOB and EAGDA in future.

10.A Widening the sources searched and reducing the scope

As much as the evidence review uncovered, it was limited due to its scoping nature and time schedule. Particularly, it resulted in the need for a methodology that was able to produce very well identified categories, but sometimes-sparse sub-categories (e.g. maladministration, human error). The value that different types of sources bring was also apparent. Indeed and as shown in Figure 7: Overlapping reporting of incidents, the highest overlap of incidents reported was six (found in the hard and soft evidence strands). Future research should shift its focus to other sources (or, of course, remain with just one of the three sources here with search terms specific to the topic under investigation), particularly to peer-reviewed journals, trade magazines and blogs. We have pursued this notion further and provide a sample of such sources, as well as giving initial search findings that could be indicative of what these could bring.

We conducted initial searches on four peer-reviewed sites, three trade magazines and eleven blogs. Four of the blogs were disregarded.[300] The search terms were:

"data AND protection AND health"

"harm AND health AND data"

"health AND data"

"biomedical AND data"

"genetic AND data"

"patient AND record"

"patient AND data"

"patient AND abuse"

As can be seen in Table 21, the number of hits generated by the search terms for all sites was 66057. Of these, 49038 emerged from the BMJ website and were not read for relevance.

[300] The blogs University of Denver Privacy Foundation Medical Patient Security, Harvard University Bill of Health and Hawktawk had no search functions. The Center for Law and the Biosciences (Stanford) archives produced zero hits.

Therefore 17019 were evaluated, and 155 were relevant. In the Appendix (see Table 28) we include a breakdown of source by each search term. For example we see potential in *BMJ News, SC Magazine* and the blogs *Hogan Lovells Chronicle of Data Protection* and *Pogowasright*.

Table 21: Alternative websites – Overview of hits and relevance

Websites searched	Hits	Relevant	Comment
Journals			
BMJ Website	49038	-	Not read for relevance
Journal of Health Organisation and Management	509	0	
BMJ News	6526	11	Some truncated after x number of articles read
BMJ Comment	7175	2	Some truncated after x number of articles read
Trade Magazines			
Computer weekly	673	3	
SC Magazine	216	66	
Professional Security	1129	23	Some truncated after x number of articles read
Blogs			
Privacy international	44	0	
Science and Society (DUKE)	20	0	
Datonomy	52	2	
BTO Solicitors	22	0	
Field Fischer Privacy and Information Law	19	0	
Hogan Lovells Chronicle of Data Protection	208	15	
Pogowasright	426	33	
Total	**66057**	**155**	

The remit of this work was extremely broad. The benefit of this is that the findings produce a sound basis to identify areas that are worthy of further, more in-depth exploration. We would therefore additionally strongly recommend that any future work have a sharper and narrower focus. Furthermore, evidence emerged from all three strands that were based on FoI requests to government departments and public authorities. Because FoI responses generally detail information not necessarily in the public domain, searching for such information alone could produce very interesting results.

10.B Future research on social constructionism

As indicated in Section 8.B.6 Quality of findings in newspapers, the research investment on the soft search was extensive. At the same time, the use to which this was put was broad. We suggest that, based on these extensive findings perhaps as a starting point only, future research examining the social construction of issues around health data misuse and abuse, and the symbiotic relationship between the media and the public would contribute to an understanding of the wider, social context of data protection.

10.C Future Research on Non-Use

A better understanding of the impact of various factors on data non-use, could be gained by conducting a prospective study on researcher views and experiences, including following through on studies from initiation. Governance challenges may differ with types of data. For example, the privacy issues in the use of free-text, omic, image, and spatial data will differ from those involved in the use of structured micro-data. It would be worth exploring these issues to understand what needs to be done to avoid non-use and to enable safe data access for research.

10.D Future research on genetic data

Given the focus of this review on health and biomedical data, and the strong implications arising from the single case involving genetic data, highlights yet another area warranting future research – and would thus fill a gap in the evidence base. As discussed in Table 22: Full details of hard evidence search, the variability with which technical terminology such as "genetic" was used in the hard evidence sources demonstrated the difficulty in locating incidents of harm with precision. Even in the more objective and arguably 'sophisticated' setting of the courts, terms such as biomedical, genetic or bioinformation were swapped for DNA and cellular samples.

As such, a narrow study focusing on genetic data would be warranted and involve expanding searches to alternative resources including peer-reviewed journals, blogs, trade magazines etc. – sources that might lend to more sophisticated (and accurate) use of technical terms such as DNA, genetic and bioinformation. Second, a *broader* approach to the search terms employed could yield more hits, and potentially more relevant hits. In broadening the scope of search terms used, one could look to known cases such as *S and Marper* identified in this review, and employ the terms adopted by the Court in substitution for e.g. genetic data. This method would begin to address the variability in how technical terms are used by the courts. The search could also be broadened if the cases *cited to* by the presiding court were then read and considered for relevancy. Applying this 'snowball' effect to the search, as opposed to sticking to the rigorous systematic approach adopted for this scoping review, would certainly offer more breadth of (more relevant) cases to consider. A similar approach on broadening both resources searched and terms employed could also be considered for a "soft" evidence review.

Finally, future research could focus on particular *uses* of genetic data and the propensity for such uses to cause harm. Particular areas of interest might lie in *new* and *unregulated* uses e.g. commercial, genetic testing for predisposition to certain diseases. By narrowing the search to a particular *use* the search would narrow the types of harms that could arise and thus identify more context-specific search terms that could then yield more relevant results.

10.E Future research on the risks, threats and vulnerabilities in processing health and biomedical data

The work undertaken in this evidence review, as well as the NCOB's previous research into the forensic use of bioinformation, has done much to identify uses of health and biomedical data that present risks to individuals, organisations and broader public interests. Whereas this evidence review focused on identifying actual instances of abuse and harm caused, future research could focus on the risks, threats and vulnerabilities that lead to such incidents. Also, whilst this report was able to comment on the implications of the evidence uncovered as to specific *motivations* that may have caused data to be abused, a narrow piece of research is warranted into preventive considerations, in order to be able to propose mitigations and practical solutions to such risks. In light of a key conclusion of this report - that current legal remedies are ineffective in compensating for abuse – carrying forward more focused research into the *risks* perpetuating such abuse is warranted.

10.F Future research and the necessity of public debate

We hope that we have demonstrated the value of public engagement throughout this report. Opening the debate to the wider public is in the spirit of citizenship. Further, we have seen the mismatch of expectations of what the protection of health and biomedical data actually is in legal terms. Not only should the public be engaged more in data security concerns regarding their own personal sensitive data, we believe that a qualitative piece of research, perhaps in the form of consultation workshops, would allow for a better understanding of these mismatches. Additionally and in focus groups, the public discuss how best the correct messages should come into the public domain.

In addition and as raised under Section 8.B.7, we found no evidence of discrimination against minority groups. Conversely, however, we found no evidence of discrimination against minority groups. In order to establish if and how minority groups might be discriminated against, it is essential to reach out to such groups via gatekeepers and gather experiential data. We believe this could produce fruitful findings.

11. Concluding thoughts

This review provides a unique legal and psychosocial framework of analysis to answer the question of whether there is any actual harm that arises from the use of health and biomedical data. This framework provides a multidisciplinary basis for conceptualising the very notion of harm as it relates to use and (perceived) abuse of data. The novel approach has provided a triangulated evidence base to answer the question and the findings indicate strongly that a more holistic understanding is required.

The holistic perspective offered in this review suggests that there are at least two types of evidence that must be considered, each with a corresponding understanding of harm. Thus, from the point of view of law and legal sanctions, and in considering the most influential legal instrument – the Data Protection Act 1998 – a hard evidence base has been generated that draws on rulings of the domestic and European courts, the First-tier Tribunal (Information Rights), and the Information Commissioner's Office. In these terms, the hard evidence frames "harm" as '…that which causes unjustifiably substantial damage or distress to the individual, which is beyond mere discomfort – physical, emotional or otherwise.'[301] This sets a high hurdle. In doing so, it fails to capture the complete picture of how individuals and social groups experience or perceive harm arising from data use and abuse.

To capture this, our soft evidence base conceptualised the notion of 'impact' arising from data use. Thus, for example, an individual might experience an impact if her/his data are used without permission, even if this is perfectly legal. Equally, organisations handling data might suffer an impact in trust and allegiance if individuals or groups whose data are held and used perceive an adverse impact through uses of which they disapprove. This is not to suggest that groundless concerns or abstract fears should drive information governance practices. Rather – as our soft evidence base suggests – the range of considerations about what might be construed as harmful is far wider than the law alone recognises. As such, the lesson is that due attention should be paid to possible impacts when using health and biomedical data, and to ensuring that governance mechanisms and actors within them have the ability to assess and, where appropriate, respond to data subjects' expectations.

Our further reliance on the social medium of Twitter has allowed us to triangulate the findings. Twitter has brought insight to the international landscape of data breaches involving health and biomedical data allowing for contrast with the UK-based evidence. Somewhat interestingly, there is less overlap between the three evidence sources than one might expect. The evidence uncovered of actual harm is modest in comparison to potential harm or to a psychosocial understanding of impacts. As stated above, the clear lack of merged or

[301] ICO, 'Preventing processing likely to cause damage or distress'.

overlapping results simultaneously indicates the limitations of the hard evidence versus, soft evidence and social media search on their own, whilst highlighting the value added by *combining* the three approaches. This allows us to derive more complete and holistic view on the types of abuses and harms at stake when processing health and biomedical data.

In all areas, the top-level message is that careless or negligence conduct – through maladministration or human error – rather than intentional and wilful abuse of data, is overwhelmingly the cause of harm/impact.

The key implication for governance is that a wider perspective on harms arising out of the use or non-use of health or biomedical data is required. This must be one that is outwith the narrow confines of the law and takes specific account of the full spectrum of harms (hard) and potential impacts (soft). In something of a closed circle of analysis, it is important to point out that the courts are already taking these considerations into account. Actual harm might be the requisite standard under the Data Protection Act, but general common law principles in breach of confidence actions and those involving human rights will account for potential harms and impacts, as well as harms to broader public interests.

Equally, this analysis of both harm and (potential) impact suggests that it is insufficient merely to ask if data controllers and other users of data have complied with the law. The human practices involved need to demonstrate sensitivity to the wider potential impacts – individual and social – that handling of health and biomedical data can bring.

APPENDICES

Table 22: Hard evidence search details

Table 23: Hard evidence incidents

Table 24: Twitter evidence incidents

Table 25: Newspaper evidence

Table 26: Impact statements from the newspaper evidence

Table 27: Reference list for newspaper articles

Table 28: Journals, trade magazines and blogs future research review

Table 22: Full details of hard evidence search

UK case law

For UK case law, the legal database LexisNexis was chosen to provide comprehensive access to all relevant judicial rulings. Courts across the whole of the UK were considered, from England, Northern Ireland, Scotland and Wales (with a detailed list of the Courts listed in Footnote 113 above). The only decisions not available in LexisNexis were those from the First-tier Tribunal (Information Rights) of the General Regulatory Chamber (formerly the Information Tribunal) which were searched for separately on the Tribunal's website.

The search conducted on LexisNexis permitted full use of Boolean search connectors. For biomedical data, broader search parameters were employed, given the lack of results following the formula used for health data – thus the search terms used were simply 'biomedical and data'.

Given the lack of results in this aspect of the search, a search for 'genetic data and breach' was undertaken. 'Genetic' data was searched for given the potential (and actual) overlap and conflation between biomedical and genetic terminology. Given the non-technical expertise and precision with which scientific terms might be used by the Courts it was desirable to expand the search for biomedical data on this basis.

First-Tier Tribunal of the General Regulatory Chamber (former Information Tribunal)

As LexisNexis did not include the decisions of the First-Tier Tribunal in its database, this search was undertaken on the Tribunal's website. The Tribunal's website did not permit Boolean search connectors, however it did allow for searches according to:

- Jurisdictional area
- Subject
- Sub-subject
- Appeal number
- Party
- Date

To give the widest yet most relevant results the only two variables chosen were jurisdictional area, and a nominated subject. Both variables were changed in order to achieve relevant results.

ICO Enforcement Actions

To complement the findings in UK case law, the ICO's enforcement of the DPA was considered. The ICO has a variety of enforcement measures at its disposal, including:

- The issuance of monetary penalty notices of up to £500,000 for serious breaches of the DPA on or after 6 April 2010
- Decision notices, which are published opinions on a public authorities' compliance with the Freedom of Information Act 2000 or Environmental Information Regulation (only applicable to England and Wales)
- Enforcement notices and 'stop now' orders to both public and private sector organisations that are in breach of the DPA, setting forth specific steps to bring themselves into compliance
- Criminal prosecutions under the DPA

Each of these enforcement measures was publicly available on the ICO's website and was considered either through an advanced search mechanism on the website, or by reading each individual case (when filtering or search options were not available).

European Court Judgments

European Court Judgments were considered due to the European basis of the UK's data protection legislation and especially in light of the relevance of European jurisprudence considering privacy implications under Article 8 of the European Convention on Human Rights. The LexisNexis database was used for this search given its comprehensive resource of all decisions of the Court of Justice of the EU (CJEU), the European Court of Human Rights (ECtHR), General Court of the EU and European Union Civil Service Tribunal (First Chamber). For the same reasoning proposed within the UK case law search, the search for biomedical data evidence was expanded to search for 'genetic or biomedical and data and breach'.

Table 23: Hard evidence incidents

(Total of 51 incidents according to criteria in hard evidence search (overlaps with soft evidence highlighted in blue)

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
UKC1	Re JR60 [2013] NIQB 93	LexisNexis, UK Case Law Database	**Unauthorised access**:	**To meet organisational objectives:** The potential for unauthorised access to health and social care records of an adult who was previously a 'Looked After Child' in Northern Ireland.	**Individual distress:** '[The applicant] does not want to be reminded of her days in care. She does not need to know in detail how her mother had let her and her sister down. In effect, she says that her time in care was a period of her life that, quite understandably, she now wants to put behind her. She wants no reminders. She is especially determined that all records of this unhappy time should not be accessed by any third parties including members of her immediate family.'
UKC2	GDC v Savery and Others [2011] EWHC 3011 (Admin)	LexisNexis, UK Case Law Database	**Unauthorised Disclosure**	**Against wishes of individual:** Use of patient medical records against and/or without patient consent	**No discussion of harm**: Except that it was against patient wishes (consent not provided) or no response.
UKC3	N (A Child) [2009] EWHC 1663 (Fam)	LexisNexis, UK Case Law Database	**Unauthorised Disclosure**	**Without safeguards:** Disclosure of confidential expert testimony/reports from psychiatrist in family law case against wishes of wife.	**Potential distress:** '...for the disclosure of such personal material would be likely to cause the mother distress and upset which would be highly likely to impact adversely upon a child living in the same household.'
UKC4	Lewis v Secretary of State for Health and another [2008] EWHC 2196 (QB)	LexisNexis, UK Case Law Database	**Unauthorised disclosure**	**Against wishes of individual/without consent:** Court authorised disclosure of documents and medical records of individuals who had died between November 1962 and August 1991 and who had, had tissues removed for analysis for the 'The Redfern Inquiry into human tissue analysis in UK nuclear facilities'.	**Potential distress:** 'It is possible that there are those who might be indirectly affected by The Inquiry's processes who do not know about it and who do not understand its implications for their deceased family member.'

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
UKC5	Re Officer O's Application for Judicial Review [2008] NIQB 52	LexisNexis, UK Case Law Database	**Unauthorised disclosure**	**Without safeguards:** Police Ombudsman requiring disclosure of medical and health records of applicant police officer under investigation following his fatal shooting of member of public with personal protection weapon. Applicant complaining that disclosures breached his right to private life. Data requested included: information in respect of the applicant's history relating to health, conduct and complaints in view of the information he received in the investigation and the applicant's assertion that his ability to recollect the events of the incident was hampered by post incident treatment from OHW.	**Damage to institution:** Of confidential relationship btw Police Officers and OHW. Mention of the officer experiencing significant emotional problems and sleep deprivation for which he was taking medication, however this was not specific to this disclosure. Thus harm was *procedural harm*, because 'the information had been taken without any reference or notice to the applicant, without affording him reasons for the decision or an opportunity to have made representations before or during the decision making process.'
UKC6	Mersey Care NHS Trust v Ackroyd [2007] EWCA Civ 101	LexisNexis, UK Case Law Database	**Unauthorised disclosure**	**By media/press:** Mr Ackroyd, is a freelance investigative journalist was passed the medical records of Mr Ian Brady (apparently from hospital staff, but never confirmed), who was incarcerated in a mental hospital for murder. On 2 December 1999, some information from these records, including verbatim extracts, was published in the Mirror in an article attributed to Gary Jones.	**Individual distress:** To patient, whose medical records disclosed in newspaper article.
UKC7	Stone v South East Coast Strategic Health Authority and others [2006] EWHC 1668 (Admin)	LexisNexis, UK Case Law Database	**Unauthorised disclosure**	**Without safeguards**: Independent inquiry into the care, treatment and supervision of Stone prior to his murder of the victims. Report would be published to world at large.	**Potential distress:** Stone was worried the public would turn more against him (that the media would sensationalise the report).

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
UKC8	Bradshaw v Chief Constable of Cambridgeshire Constabulary [2006] All ER (D) 217	LexisNexis, UK Case Law Database	**Unauthorised disclosure**	**Against wishes of individual:** Claimant wanted third party's confidential medical and personnel records disclosed in court for his proceedings against his employer - the 3rd party medical records in question were to help show stress-related sick leave and to establish foreseeability for negligence of the ER.	**Potential distress:** Harm to the 3rd party not clearly mentioned - except that he clearly opposed to his medical records being used - possibility of further distress - comments such as the third party had 'a lot of problems' and already had to take leave off work for stress etc.
UKC9 (Also in Te09)	Henry v British Broadcasting Corporation - [2005] All ER (D) 43	LexisNexis, UK Case Law Database	**Falsification/fabrication of data**	**To meet NHS targets:** Libel action re: BBC news feature on falsification of hospital waiting times - did BBC have a qualified privilege to publish.	**Harm to broader public interests and potential distress**: The NHS suffered a loss of public trust due to the falsifying of waiting times. Further, '[a]lthough there was no evidence that the health of any particular patient had suffered by reason of the waiting list fraud, that was likely to have been the result in the cases of some of those whose treatment had been delayed.'
UKC10	R (on the application of E) v Bristol City Council [2005] EWHC 74 (Admin),	LexisNexis, UK Case Law Database	**Unauthorised disclosure**	**Against wishes of individual:** Notifying claimant's sister, as nearest relative, against claimant's wishes, re: her mental health problems, history etc.	**Potential distress**: 'The claimant does not want her sister involved with her or her mental health problems, and/or her care at all. I accept that there is credible evidence that if Mrs S is involved in decisions relating to the claimant's admission for an assessment or treatment, and/or if Mrs S were to take any action under the Mental Health Act 1983 in respect of the claimant, that that would cause the claimant significant distress.'
UKC11	Campbell v MGN Ltd. [2004] UKHL 22	LexisNexis, UK Case Law Database	**Unauthorised disclosure**	**By media/press**: The publication re Naomi Campbell's drug addiction and treatment in NA went beyond disclosure which was necessary to add credibility to the legitimate story that the claimant had deceived the public and went beyond the journalistic margin of appreciation allowed to a free press; that although the photographs of the claimant were taken in a public place, the context in which they were used and linked to the articles added to the overall intrusion into the claimant's private life.	**Potential distress**: 'A person in her position would find disclosure highly offensive, and might also be deterred from continuing with the therapy, thereby causing a setback to recovery'.

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
UKC12	Re B (Disclosure to other parties) [2001] All ER (D) 22 (Aug) FCR 32	LexisNexis, UK Case Law Database	**Unauthorised disclosure**	**Against wishes of individual:** Husband asked to see psychiatrist, psychologist and therapist records of wife and two children in violation of their Art 8 right to privacy.	**Potential distress:** 'Knowledge of R (abusive husband) having access to that material would be deeply distressing for the mother and the children, and would be wholly disproportionate to any legitimate forensic purpose that would be served by allowing R to see it.'
UKC13	A Health Authority v X and others [2001] 2 FCR 634, All ER (D) 132	LexisNexis, UK Case Law Database	**Unauthorised disclosure**	**Against wishes of individual**: Health authority seeking disclosure of medical records in order to carry out investigation against objections of patients.	**No discussion of harm**
UKC14	R v Department of Health, ex parte Source Informatics Ltd [2001] QB 424, [2000] 1 All ER 786	LexisNexis, UK Case Law Database	**Unauthorised disclosure**	**Against wishes of individual**: S Ltd wished to collect data on the prescribing habits of general practitioners (GPs), which it planned to sell to pharmaceutical companies so that they could market their products more effectively. It therefore asked pharmacists, for a small fee, to provide it with certain information contained on prescription forms, namely the names of GPs and the identity and quantity of drugs that they prescribed, but not the names of patients.	**No harm:** If anonymised data was used – even if used for a commercial purpose and without the prior notice of this use – no harm could be caused to the patients.
IT1	Pauline Bluck v IC EA/2006/0090	UK Information Tribunal Cases	**Unauthorised disclosure**	**FOI claim**: The NHS would breach the duty of confidence owed to Karen Davies if it disclosed the Medical Records to the deceased's Mother, other than under the terms of the FOIA (with consent of her widower/next of kin) and that the breach would be actionable by the personal representatives of Karen Davies.	**Harm to institution:** Trust in the confidential nature of the doctor/patient relationship will be diminished and thus harmed if a patient believed that his or her information might be disseminated to the public after their death.

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
ICOP1	03/12/2013 Maidstone Magistrates Court	UK ICO Prosecutions	**Unauthorised access**	**Without clinical or legitimate justification:** Unlawfully accessing the medical records of approximately 1,940 patients registered with the surgery. Unlawfully obtaining or accessing personal data is a criminal offence under section 55 of the Data Protection Act 1998. The offence is punishable by way of 'fine only' - up to £5,000 in a Magistrates Court or an unlimited fine in a Crown Court.	**No discussion of harm**: However, was fined a total of £996 and ordered to pay a £99 victim surcharge and £250 prosecution costs.
ICOP2	23/05/2013 West Hampshire Magistrates Court	UK ICO Prosecutions	**Unauthorised access**	**Without clinical or legitimate justification:** A former manager of a health service based at a council-run leisure centre in Southampton has been prosecuted by the ICO for unlawfully obtaining sensitive medical information relating to over 2,000 people. Paul Hedges took the information hoping to use the data for a new fitness company he was setting up.	**Individual distress:** 'The council became aware of their former employee's actions when they received complaints about patients being approached by Mr Hedges; who had since set up a similar service using the Active Options name and branding.' In addition, he was fined £3,000 and ordered to pay a £15 victim surcharge and £1,376 prosecution costs.
ICOP3	12/03/2013 West Hampshire Magistrates	UK ICO Prosecutions	**Unauthorised access**	**Without clinical or legitimate justification:** Former receptionist at GP office unlawfully obtaining sensitive medical information relating to her ex-husband's new wife. Accessed the information on 15 separate occasions over a 16-month period while working as a receptionist at the Bath Lodge Practice. The breach became apparent after Phillips left her job and sent a text message to her ex-husband's partner referring to highly sensitive medical information taken from her medical record.	**Individual distress:** New wife was harassed by the ex-wife referring to highly sensitive medical information taken from her medical record. In addition, she was fined £750 and ordered to pay a £15 victim surcharge and £400 prosecution costs.

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
ICOP4	12/01/2012 Liverpool City Magistrates Court	UK ICO Prosecutions	**Unauthorised access**	**Without clinical or legitimate justification**: A former health worker has pleaded guilty to unlawfully obtaining patient information by accessing the medical records of five members of her ex-husband's family in order to obtain their new telephone numbers.	**Individual distress:** The defendant's father-in-law contacted the hospital after receiving nuisance calls that he suspected were made by his former daughter-in-law. Having changed his phone number in July 2009 following unwanted calls from Ms Kechil, he was immediately concerned that there had been a breach of patient confidentially. She was fined £500 and ordered to pay £1,000 towards prosecution costs and a £15 victim surcharge.
ICOM1 (Also in In09, G28 and Ti08)	British Pregnancy Advice Service 7 March 2014	UK ICO Monetary Penalties	**Technical security breach**	**Third party:** A hacker threatened to publish thousands of names of people who sought advice on abortion, pregnancy and contraception. BPAS retained call back information unnecessarily of 9,900 people which accessible to the hacker. BPAS also did not store passwords securely or ensure communications secure.	**Potential distress - emotional and physical:** Some of the call back details were from individuals whose ethnicity and social background could have led to physical harm or even death if the information had been disclosed by the attacker.
ICOM2	North East Lincolnshire Council 29 Oct 2013	UK ICO Monetary Penalties	**Lost hardware**	**Human error:** An unencrypted USB memory stick containing personal and sensitive personal data was lost on the data controller's premises.	**Potential distress (physical and emotional):** Following the incident, the data controller carried out a risk assessment for the potential damage and distress to the data subjects. The internal report estimated that the loss of the sensitive personal data is likely to lead to the ill health of those affected through the disclosure of the data or due to a break in the services, which they were receiving. The likely damage and distress to the data subjects is substantial due to the volume of data which has been lost, and that the data subjects are children aged 5 -16, some of whom are deemed vulnerable (and their families). The data subjects were not notified of the data breach.
ICOM3 (Also G07)	NHS Surrey 12 July 2013	UK ICO Monetary Penalties	**Non-secure disposal of hardware**	**Maladministration**: In decommissioning hard drives, did not properly vet the 3rd party vendor and thus personal data belonging to thousands of patients on hard drives sold on an online auction site.	***Potential* for individual distress:** Approximately 1570 hard drives holding confidential sensitive personal data relating to an unknown number of patients and staff; The majority of the hard drives sold on the internet have not been recovered

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
ICOM4 (Also TW23)	North Staffordshire Combined Healthcare NHS Trust 13 June 2013	UK ICO Monetary Penalties	**Unauthorised disclosure**	**Human error:** North Staffordshire Combined Healthcare NHS Trust, after several faxes containing sensitive personal data were sent to a member of the public in error.	***Potential* for individual distress:** because the ICO could not obtain confirmation that the member of the public destroyed the SPD received, potential in future for this information to be used to the disadvantage/detriment of the patients.
ICOM5	Stockport Primary Care Trust 3 June 2013	UK ICO Monetary Penalties	**Non-secure disposal of paper file**	**Maladministration**: Stockport Primary Care Trust fined following the discovery of a large number of patient records at a site formerly owned by the Trust by the purchaser of the site.	***Potential for* Individual distress:** because some of the data subjects were known to the purchaser who accessed the information thus causing embarrassment etc.; and data disclosed to a wider circle of people - five prospective purchasers had access to the site in total.
ICOM6 (Also in B05)	Nursing and Midwifery Council 15 February 2013	UK ICO Monetary Penalties	**Lost hardware**	**Human error**: Nursing and Midwifery Council. The council lost three DVDs related to a nurse's misconduct hearing, which contained confidential personal information and evidence from two vulnerable children. An ICO investigation found the information was not encrypted.	**Potential for individual distress:** just that DVDs were never found (and thus potential for future use of SPD remains).
ICOM7	London Borough of Lewisham 12 December 2012	UK ICO Monetary Penalties	**Loss of paper files**	**Human error:** a social worker left sensitive documents in a plastic shopping bag on a train, after taking them home to work on. The files, which were later recovered from the rail company's lost property office, included GP and police reports and allegations of sexual abuse and neglect.	***Potential* for individual distress:** If disclosure resulted in extensive media coverage about individuals' personal lives; and potential to disrupt on-going legal case data related to the data in question.
ICOM8	Devon County Council 10 December 2012	UK ICO Monetary Penalties	**Unauthorised disclosure**	**Human error**: Devon County Council social worker used a previous case as a template for an adoption panel report they were writing, but a copy of the old report was sent out instead of the new one. The mistake revealed personal data of 22 people, including details of alleged criminal offences and mental and physical health.	**Individual distress:** The parents of the child being considered for adoption complained to ICO about the distress they had suffered; the unauthorised third parties did not return the report for 2 months.

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
ICOM9	Stoke-on-Trent City Council 25 October 2012	UK ICO Monetary Penalties	**Unauthorised disclosure**	**Human error:** A solicitor employed by the data controller was working on a child protection case and sent 11 emails (intended for Counsel instructed on the case) to the wrong email address by mistake. The emails varied in sensitivity but some of them contained confidential and highly sensitive personal data about the non-accidental injuries sustained by a child together with medical information relating to two adults and two children.	**Potential for harm**: The 11 emails containing confidential and highly sensitive personal data were sent to a live email address via the internet and have not been recovered - importantly (to ICO): To the Commissioner's knowledge the personal data involved has not been accessed or further disseminated and the security breach did not affect the child protection proceedings.
ICOM10 (Also in G10)	Torbay Care Trust 6 August 2012	UK ICO Monetary Penalties	**Unauthorised disclosure**	**Maladministration:** A monetary penalty of £175,000 was issued to Torbay Care Trust after sensitive personal information relating to 1,373 employees was published on the Trust's website. (Data publicly available for over 19 weeks, this file receiving 300 visits)	**Potential financial harm:** risk for identity theft and thus financial loss.
ICOM11	St George's Healthcare NHS Trust 12 July 2012	UK ICO Monetary Penalties	**Unauthorised disclosure**	**Human error**: A monetary penalty of £60,000 was issued to St George's Healthcare NHS Trust after a vulnerable individual's sensitive medical details were sent to the wrong address. (Patient had not lived there for five years)	**Potential Distress:** ICO considered it likely to cause substantial individual distress and would prejudice any criminal prosecution
ICOM12	Belfast Health and Social Care Trust 19 June 2012	UK ICO Monetary Penalties	**Non-secure disposal of data**	**Maladministration:** Confidential and sensitive personal data consisting of patient and staff records (some dating from the 1950s) were stored in one of the disused sites, namely Belvoir Park Hospital (the "site"). Whilst, CCTV used at first, 'CCTV system monitoring the main entrance was not recording and the fire and intruder alarms had been isolated after developing faults.' Trespassers gained access to the site on several occasions to photograph the records, which were then posted on the internet.	**Potential distress:** The contravention was of a kind likely to cause substantial distress to the data subjects and complaints were made by some of the affected individuals.

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
ICOM13 (Also in B09, E02, E09, E10, In06, Ma12)	Brighton and Sussex University Hospitals NHS Trust 1 June 2012	UK ICO Monetary Penalties	**Non-secure disposal of hardware**	**Maladministration:** In decommissioning hard drives, did not properly vet the 3rd party vendor and thus personal data belonging to thousands of patients on hard drives sold on an online auction site, including data re: HIV positive patients.	**Potential harm to individuals:** All the hard drives have not been recovered and that the data was extremely sensitive (re: HIV positive status) makes it likely the data could be misused in future to discriminate against them or otherwise cause harm.
ICOM14	Central London Community Healthcare NHS Trust 21 May 2012	UK ICO Monetary Penalties	**Unauthorised disclosure of data**	**Maladministration:** Sensitive personal data was faxed to an incorrect and unidentified number. The contravention was repeated on 45 occasions over a number of weeks and compromised 59 data subjects' personal data. (Data re: patients receiving palliative care at the time of the security breach).	**Potential distress:** ICO considered it 'likely to cause substantial distress to the patients' although no complaints received from data subjects.
ICOD1	3 September 2013, FOI Decision Notice re: Walsall Clinical Commissionin g Group	UK ICO Decision Notice	**Unauthorised disclosure**	**FOI request**	**Potential distress:** Disclosure of the data re: removal of the tattoos, from what body part etc. would have 'significant impact on the mental health of data subjects'.
ICOD2	21 August 2013, FOI Decision Notice re: Norfolk and Suffolk Probation Trust	UK ICO Decision Notice	**Unauthorised disclosure**	**FOI request**	**Potential: distress:** Disclosure of the data re: complaints made about an NHS nurse, which would include info on her physical health would: 'Disclosure of this type of information is likely to have a highly distressing effect on the data subject."
ICOD3	17 January 2013, FOI Decision Notice re: East Herts Council	UK ICO Decision Notice	**Unauthorised disclosure**	**FOI request**	**Potential distress (detriment to physical health):** Disclosure of data re: why the CEO left office, which was for health reasons, would increase the risk "to causing damage or distress to the health of the data subject." "A real risk that disclosure of the information might exacerbate the former Chief Executive's health situation and have a detrimental effect upon her well- being."

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
ICOD4	5 March 2012, FOI Decision Notice re: Dr Barbara Allan, Dr Matthew Joslin, and Dr Tim Worden ("The Docs")	UK ICO Decision Notice	**Unauthorised disclosure**	**FOI request**	**Potential distress and damage to institution**: Disclosure of the data re: the Dr's absences would 'likely to have four adverse effects. Firstly, it would erode their trust and confidence in their fellow partners doing what it said it would with their personal HR data. Secondly, it would reveal information from which one can derive information about the health or otherwise of the individual and where the default expectation is that health data would be kept confidential, the individual would have their expectations not recognised. Thirdly, the practice considered that the data subject would not expect that this information would be provided to enable the complainant to pursue them further. Fourthly, the practice explained that it was based in a small community and the wider dissemination of the information could lead to speculation about the doctor's Fitness to Practice, whether accurate or not.'
EUC1	Z v Finland (19970 25 EHRR 371, 405 at para 95	LexisNexis EU Case Law Databases	**Unauthorised disclosure**	**By press/media:** A Court of Appeal judgment revealed Z's identity (wife of X, on trial for rape and manslaughter) and HIV-positive status without any 'cogent' reasons. (see para 113 of the judgment). Whilst ultimately the identity of Z and her HIV-positive status was disclosed by Finland's largest newspaper, this made possible by the Finnish Court of Appeal who faxed the newspaper their judgment which confirmed her identity and HIV-status.	**Individual distress and potential harm to broader public interest: '**The publication of the information concerned gave rise to a violation of the applicant's right to respect for her private and family life as guaranteed by art 8.**'** (see para 113 of judgment) Furthermore, 'The court [found] it established that the applicant must have suffered non-pecuniary damage as a result of the disclosure of her identity and medical condition in the Court of Appeal's judgment. Finally, the Court recognised the great potential for harm to broader public interests – disclosure of such sensitive health data can '…discourage persons from seeking diagnosis or treatment and thus undermine any preventive efforts by the community to contain the pandemic.' (para 96)
EUC2	Earl Spencer v United Kingdom (1998) 25 EHRR	LexisNexis EU Case Law Databases	**Unauthorised disclosure**	**By press/media:** the publication of private information about the applicants' marriage and medical condition and photographs taken with a telephoto lens (relating to bulimia and mental health problems of Countess Spencer - photos of her on grounds of private health clinic).	**Individual distress:** emotional and physical - "great personal distress" caused to the applicants, the consequent strain on their relationship and the effect on the second applicant's treatment.

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
EUC3	McGinley and another v United Kingdom [1998] ECtHR	LexisNexis EU Case Law Databases	**Non-use of data**	**For organisational objectives:** Withholding of documents, which would have helped applicants that were stationed on or near Christmas Island at the time of nuclear tests in 1958. This info would have helped them ascertain whether there was a link between their health problems and exposure to radiation. Internal UK government reasons (not-disclosed) as reason for not disclosing.	**Individual distress:** The issue of access to information which could either have allayed their fears or enabled them to assess the danger to which they had been exposed, was sufficiently closely linked to their private and family lives within the meaning of Article 8 as to raise an issue under that provision; Given the fact that exposure to high levels of radiation is known to have hidden, but serious and long-lasting, effects on health, it is not unnatural that the applicants' uncertainty as to whether or not they had been put at risk in this way caused them substantial anxiety and distress.
EUC4	MS v Sweden (1999) 28 EHRR 313	LexisNexis EU Case Law Databases	**Unauthorised access**	**Against the wishes of the individual:** Patient's records disclosed for purpose of assessing social security claim. Importantly: 'It did not follow from the fact that she had sought treatment at the clinic that she would consent to the data being disclosed to the Office' for the purposes of her workers compensation claim.	**Individual distress:** The individual suffered individual distress because of a violation of her Article 8 Rights (under the ECHR) to the respect of private life. The medical records contained highly sensitive and personal data regarding a previous abortion, and were used for an entirely different purpose, without her consent.
EUC5	Armoniene v Lithuania (App no 36919/02) - [2008] ECHR 36919/02	LexisNexis EU Case Law Databases	**Unauthorised disclosure**	**By press/media:** The respondent state's biggest daily national newspaper published an article which stated that the applicant's husband was HIV-positive and that he was the father of two children by another woman who was also suffering from AIDS.	**Individual distress and financial harm:** The family had to move from their village. The newspaper article had humiliated the husband and the publication of information about his private life had caused him non-pecuniary damage, had an impact on his health, and a negative influence on his family life and his reputation as well as restricting his family's opportunities to interact with others. He died and wife brought suit based on such harms/damages.
EUC6	Biriuk v Lithuania (App no 23373/03) [2008] ECHR 23373/03	LexisNexis EU Case Law Databases	**Unauthorised disclosure**	**Maladministration:** Press disclosed HIV/AIDS status of woman, which was confirmed by hospital staff.	**Individual distress:** Publication had humiliated her and caused her significant non-pecuniary damage.

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
EUC7	S and Marper v United Kingdom (2009) 48 EHRR 50	LexisNexis EU Case Law Databases	**Unauthorised retention**	**Maladministration**: DNA profiles and fingerprints were being retained indefinitely without regard to the nature or gravity of the offence with which the individual was originally suspected of or their age; there existed only limited possibilities for an acquired individual to have their data removed from the nationwide database or destroyed.	**Individual distress:** 'The retention of the first applicant's data was to be considered especially harmful given his special situation as a minor and the importance of his development and integration in society'.
EUC8	Szuluk v United Kingdom (App. No. 36936/05) - [2009] All ER (D) 02 (Jun) (ECtHR)	LexisNexis EU Case Law Databases	**Unauthorised access**	**Without clinical or legitimate justification**: Requirement that claimant's medical correspondence be read by prison medical officer	**Individual distress and suboptimal clinical care:** He was concerned that his attempts to confirm that he was receiving adequate treatment in hospital might be regarded by the prison medical officer as criticism and that this might inhibit his relationship with his external medical specialist. The applicant further contended that there was an obvious risk that monitoring of medical correspondence would inhibit what a prisoner conveyed, thereby harming the quality of advice received.

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
EUC9	I v Finland (2009) 48 EHRR 31	LexisNexis EU Case Law Databases	**Unauthorised access**	**Insufficient safeguards**: Early in 1992, the applicant began to suspect that her colleagues were aware of her HIV positive status. She was a nurse at the same hospital she was receiving treatment from. At that time, hospital staff had free access to the patient register, which contained information on patients' diagnoses and treating doctors. Thus, the claim was based on the failure of the hospital 'to guarantee the security of her data against unauthorised access, or, in Convention terms, a breach of the State's positive obligation to secure respect for her private life by means of a system of data protection rules and safeguards.' (para 37) (However, 'The Court of Appeal found that the applicant's testimony about the events, such as her colleagues' hints and remarks beginning in 1992 about her HIV infection, was reliable and credible. However, it did not find firm evidence that her patient record had been unlawfully consulted (see para 15).	**Individual distress:** The Court awarded I ERU 8,000 for individual distress caused by the need to change her place of work and the fact that the rumours about her HIV infection had affected her son's life. (She claimed for financial damages as well, but these were not awarded – these claims included compensation for the hospital 'refusing' to renew her employment contract and thus her subsequent unemployment; having to move house because of the rumors regarding her HIV status).
EUC10	Gillberg v Sweden (App no 41723/06) [2010]	LexisNexis EU Case Law Databases	**Non-use of data**	**Misinterpretation of legal obligations**: Professor was a university professor (G) and complained that his conviction for misuse of office was in breach of the European Convention on Human Rights 1950 art.8 and art.10. G was director of the university's Department of Child and Adolescent Psychiatry. He had refused requests from a sociologist (K) and a paediatrician (E) for access to confidential information, which formed part of a research project, claiming that he had promised absolute confidentiality to the families of the children concerned.	**No discussion on harm:** Rather, a discussion about *interference with rights* – the *non*-use of data would impinge on K and E's rights under art.10, as granted by the Court of Appeal, to receive information in the form of access to the documents concerned and, under art.6, to have the court's judgments implemented.

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
EUC11	P and another v Poland (App. No. 57375/08) [2012] ECHR 57375/08	LexisNexis EU Case Law Databases	**Unauthorised disclosure**	**Maladministration:** P had become pregnant after being brutally raped. She made an early decision to terminate the pregnancy. When seeking an abortion, the hospital issued a press release regarding her situation, causing P's circumstances to become national news.	**Individual distress and suboptimal clinical care:** P became subject of national news media frenzy. She received texts from various unknown third parties harassing her. Upon discharge from the hospital, she was harassed by onlookers waiting outside. She was eventually forced to have the abortion 500km from home.
EUC12	Mitkus v Latvia (App. No. 7259/03) [2012] ECHR 7259/03	LexisNexis EU Case Law Databases	**Unauthorised disclosure**	**By media/press:** The newspaper could have informed the public about the pending proceedings concerning the alleged negligence of the medical staff at Central Prison without publishing his picture, without the article losing much of its informative value, if any at all.	**Individual distress:** the respondent and requesting non-pecuniary damages for moral and psychological harm caused to him when Rīgas Balss published the above-mentioned article, which included his photo in which he was fully recognisable. The applicant has furthermore indicated to the Court that as a result of the publication of the disputed article he was ostracised by other prisoners because of the information about his HIV infection
EUC13	Avilkina and others v Russia (App. No. 1585/09) - [2013] ECHR 1585/09	LexisNexis EU Case Law Databases	**Unauthorised disclosure**	**Without consent of individuals/against wishes**: Prosecutor's office instructing medical institutions to report incidents of refusal of transfusion of blood by members of religious organisation – information contained in applicants' medical files - without their consent.	**No discussion of harm:** However discussion re: lack of proportionality and consideration of individual rights - the means employed by the prosecutor in conducting the inquiry did not need to be so oppressive for the applicants. There were options, other than ordering the disclosure of confidential medical information, available to the prosecutor to follow up on the complaints lodged with his office. In particular, he could have tried to obtain the applicants' consent for the disclosure and/or questioned them in relation to the matter. Nevertheless, the prosecutor chose to order the disclosure of the confidential medical information without giving the applicants any notice or an opportunity to object or to agree

Incident No.	Case Name and Date	Source	Abuse Type	Abuse Cause	Harm
EUC14	Ageyevy v Russia - (2013) 34 BHRC 449	LexisNexis EU Case Law Databases	**Unlawful disclosure**	**Maladministration:** The hospital and health authorities disclosed to third parties data concerning G that was medical, personal and sensitive, including his name, photographs containing, among other things, information of a medical character, and his detailed medical diagnosis and also authorised direct access of TV crews to G who was only three years old at the time and was not accompanied by his parents. Given that the authorities did not seek from the media involved any guarantees concerning the non-disclosure of G's identity, and in view of the subsequent coverage of the events, which included the widespread dissemination of all of the mentioned data, the relevant information was in fact released to the public at large.	**Individual distress and financial harm:** The applicants claimed compensation in the amount of 140,940 euros (EUR) in respect of their alleged pecuniary losses because of the loss of the first applicant's job in a bank, which allegedly resulted from the publication in the media of the events in the present case. The Court considers that the applicants must have sustained stress and frustration as a result of the violations found. Making its assessment on an equitable basis, the Court awards the first applicant EUR 25,000 and the second applicant EUR 30,000 in respect of non-pecuniary damage, plus any tax that may be chargeable.

Table 24: Social media evidence of health or biomedical data abuse internationally

70 incidents according to Twitter search criteria – overlaps with soft evidence highlighted in light blue, with hard evidence highlighted in dark blue.

Incident No.	Date	Location	Abuse Type	Abuse Cause	Harm
TW1 (Also on Ma18)	25-Mar-14	US	**Technical security failure**	**Maladministration:** Stanford hospital and clinics and one of its former contractors allowed the medical information of 20,000 emergency room patients to be posted online for nearly a year.	**No direct mention of harm:** However, there is a possibility for a $4.1M settlement, equating to victims receiving $100/each.
TW2	25-Mar-14	USA	**Loss of hardware:**	**Human error**: A computer flash drive containing limited patient information on 586 children treated at Orlando Health's Arnold Palmer Medical Center was misplaced and treated as a data security breach.	**No direct mention of harm:** however began contacting affected patients; they say no evidence that data was used.
TW3	21-Mar-14	US	**Unauthorised disclosure**	**Human error**: Marian Regional Medical Center (part of Dignity Health) in California recently notified patients that electronic files with "limited patient information" was sent to the wrong contracted health insurance plan during the first week of March. The agent who received it promptly notified MRMC and the file was sent back.	**No direct mention of harm**
TW4	21-Mar-14	US	**Theft**	**Third Party:** The University of California San Francisco reports data breach after desktop computers stolen – personal & medical info for 9,000 patients compromised.	**Potential for financial harm:** 'Information and assistance is being offered to those affected, and credit monitoring is being offered to those whose Social Security numbers were involved, officials said.'
TW5	21-Mar-14	US	**Technical security failure**	**Third Party:** The number of UPMC employees that have been affected by a recent data breach at the University of Pittsburgh Medical Center now stands at 322. The breach allowed someone to use the employees' and patients' personal information to electronically file fraudulent income tax returns.	**Individual distress and financial harm**: Fraudulent tax returns filed based on information hacked, resulting in detriment to individual's credit rating.
TW6	19-Mar-14	US	**Technical Security Failure**	**Third Party:** Someone hacked the computers of a state-licensed provider of services to the developmentally disabled and stole Social Security numbers and medical information for about 9,700 clients.	**Potential for financial harm**: they are offering credit-monitoring services to victims.

Incident No.	Date	Location	Abuse Type	Abuse Cause	Harm
TW7	19-Mar-14	US	**Theft**	**Third Party:** The Dec. 2009 theft of laptops belonging to AvMed, a Florida-based health insurer, exposed the patient records of tens of thousands of its customers. Several victims later filed a putative class action lawsuit against AvMed.	**No harm:** The victims of data breach ' suffered no direct losses or identity theft from the breach but nevertheless accused AvMed of negligence, breach of contract, breach of fiduciary duty and unjust enrichment' and were still awarded a $3M settlement - 'The settlement is believed to be the first in which victims of a data breach are compensated without having to show they suffered any losses from the theft of their personal data'.
TW8	19-Mar-14	US	**Technical security failure**	**Maladministration:** A company that provides medical transcription services has agreed to settle Federal Trade Commission charges that its inadequate data security measures unfairly exposed the personal information of thousands of consumers on the open Internet, in some instances including consumers' medical histories and examination notes.	**Potential for individual harm (distress and financial)**: FTC brings such claims on the basis of the company being involved in fraudulent, deceptive, and unfair business practices. Can assume individual or financial distress because of nature of information lost: the data was indexed by a major internet search engine and were publicly available to anyone using the search engine. Some of the files contained notes from medical examinations of children and other highly sensitive medical information, such as information about psychiatric disorders, alcohol use, drug abuse, and pregnancy loss.
TW9	19-Mar-14	US	**Theft**	**Third Party:** Los Angeles county and its contractor, experienced a theft of medical data on 165,000 patients. The data may have included patients' names, Social Security numbers, and medical and billing information, birth dates, addresses and diagnoses. The data was stolen from a company hired by LA county to handle billing and collections. The suit alleges the company and the county did not notify affected patients in a timely fashion and that more stringent protection of private data is required.	**Individual distress and potential financial harm**: individuals credit at risk - furthermore considered harmful that county did not notify victims.
TW10	18-Feb-14	US	**Technical security failure**	**Third Party:** Minnesota's Olmsted Medical Center recently began notifying more than 500 former employees that their personal information may have been exposed via hacker.	**Potential for financial harm:** no evidence of harm, but victims offered credit monitoring.

Incident No.	Date	Location	Abuse Type	Abuse Cause	Harm
TW11	06-Feb-14	US	**Loss of paper files**	**Human error**: Some missing operating room schedules may have resulted in the disclosure of patient information for 874 people.	**Potential for financial harm**: no evidence of harm, but victims offered credit monitoring.
TW12	24-Jan	US	**Technical security failure**	**Maladministration**: On December 12, Sidney Regional Medical Center learned that a previous version of their web site had been stored on a server without proper settings to block indexing by search engines. The mistake was discovered by a former applicant who was Googling her own name.	**Potential for financial harm**: no evidence of harm, but victims offered credit monitoring.
TW13	27-Dec-13	US	**Technical security failure**	**Maladministration**: A LabMD spreadsheet with Social Security numbers, medical codes and other information, about more than 9,000 people, was found on an online file-sharing network last year.	**No direct mention of harm**
TW14	14-Dec-13	US	**Technical security failure**	**Maladministration**: A dental clinic discovered 1,000s of their patients' data online.	**No direct mention of harm**
TW15	04-Dec-13	US	**Theft**	**Self-gain**: A former Owensboro Medical Health System (of Kentucky) employee, Ilene W. Bullington, sold patient information from February 2010 and August 2012.	**Financial harm**: She used patient information such as names, birth dates and Social Security numbers to obtain financial loans that fluctuated from $300 to $7,000 (using other's identities).
TW16	24-Nov-13	US	**Technical security failure**	**Third Party:** A teenager was suspected of hacking into the Sachem school district computer system, accessing student records that included Social Security numbers and confidential medical information. Calicchio posted the information on a website provided by 1Apps.com, and Sachemunspun.com, a community forum.	**No direct mention of harm**
TW17	06-Nov-13	US	**Theft**	**Maladministration**: Two laptops from an administrative office of the hospital group AHMC Healthcare Inc. ("AHMC") in Alhambra, California were stolen. This compromised the health data of approximately 729,000 individuals. Although the laptops were password protected, they were unencrypted.	**Potential for financial harm**: they suggest credit monitoring by victims.

Incident No.	Date	Location	Abuse Type	Abuse Cause	Harm
TW18	18-Oct-13	US	**Theft**	**Maladministration:** A data breach at the University of California Los Angeles (UCLA) exposed the personal information of more than 16,000 patients of the UCLA Health System. In September 2011, an external hard drive containing personal information of 16,288 UCLA patients was stolen from the home of a doctor working with the UCLA Faculty Group. The records dated from July 2007 through July 2011. The patient information on the lost hard drive was encrypted, but a piece of paper that had the password to decode the data also went missing.	**No direct mention of harm**
TW19	28-Sep-13	US	**Theft**	**Maladministration**: A laptop with unencrypted patient information was stolen from the Audiology Department at Santa Clara Valley Medical Center. The laptop was used for hearing screenings and as such, contained patients' name, medical record number, date of birth, gender, date of service, and "brainwaves from testing".	**No direct mention of harm**
TW20	07-Sep-13	US	**Theft**	**Maladministration**: Four unencrypted computers were stolen, which contained personal information on four million individuals. Included health insurance data, medical diagnoses and record numbers.	**No direct mention of harm**
TW21	12-Jul-13	US	**Unauthorised access**	**Without clinical or legitimate justification**: The private information of nearly 3,000 Long Beach Memorial Medical Center patients may have been breached by an employee, including insurance information and the reason for admission.	**Potential for financial harm:** they are offering credit-monitoring services to victims.
TW22	27-Jun-13	US	**Technical Security Failure**	**Third Party:** Florida's Sight and Sun Eyeworks Gulf Breeze recently began notifying 9,000 patients that their personal information had been accessed inappropriately. In a statement on its Web site, Sight and Sun stated that patients' names, addresses, Social Security numbers and medical records were accessed and copied.	**No direct mention of harm**: Although, former employees Dr. Suzanne M. Day and Lynette Bramlett took patient data with them in order to solicit patients when they left to work for a competing optometry office.

Incident No.	Date	Location	Abuse Type	Abuse Cause	Harm
TW23 (Also in ICOM4)	19-Jun-13	UK	**Unauthorised disclosure**	**Human error:** North Staffordshire Combined Healthcare NHS Trust was fined £55,000 following a breach of the Data Protection Act that resulted in the exposure of three patients' medical information. Employees of the Trust mistakenly sent 3 faxes to members of the public, including details on physical and mental health.	**No direct mention of harm**
TW24	26-May-13	US	**Non-secure disposal of paper files**	**Maladministration:** El Centro Regional Medical Center (ECRMC) was notified that the x-rays ECRMC had provided to a trusted vendor for digitization and destruction were missing from a storage warehouse and may not have been properly destroyed.	**Potential for financial harm:** they are offering credit-monitoring services to victims.
TW25 (Also in B4)	25-Apr-13	UK	**Non-secure disposal of paper files**	**Maladministration:** An investigation has been launched into how confidential medical records were found in a garden in Londonderry. The Western Health Trust has confirmed that the documents contained "sensitive personal information" and said it had reported the breach to the Information Commissioner's office. The details of 13 women and four men were on eight A4 sheets of papers," he said. "There are a few lines on each and they go into intimate detail about their treatment, condition and their past history."	**No direct mention of harm**
TW26	13-Apr-13	US	**Theft**	**Maladministration:** Oregon Health & Science University reported that a surgeon's unencrypted laptop was stolen from a vacation rental home in Hawaii. The stolen laptop contained medical record numbers, types and dates of surgeries, names of surgeons of 4,022 patients, and (worst of all) the Social Security numbers for at least 17 confirmed patients.	**Potential for financial harm:** they are offering credit-monitoring services to victims.
TW27	12-Apr-13	US	**Loss of hardware:**	**Maladministration**: The William Jennings Bryan Dorn VA Medical Center in Columbia, S.C., has informed 7,405 patients about a recent data breach. The breach involves an unprotected laptop containing patient names, birth dates, respiratory test results and partial Social Security numbers. The laptop is yet to be found.	**Potential for financial harm:** they are offering credit-monitoring services to victims.

Incident No.	Date	Location	Abuse Type	Abuse Cause	Harm
TW28	08-Apr-13	US	**Technical security failure**	**Maladministration:** Thousands of patients of a New York state hospital had their medical records exposed when they were left unprotected on a third party server for several months.	**Potential for individual distress:** Auditors concluded that some patient records may have been accessed or downloaded by intruders, thus with potential for individual distress.
TW29	29-Mar-13	US	**Loss of hardware:**	**Maladministration**: The University of Mississippi Medical Center is notifying patients, who visited between 2008 and January 2013, that their health information may have been stored on a laptop computer that's "missing". Apparently, the device was not protected with laptop encryption like AlertBoot, which may have been a result of the laptop being "a shared device, used by clinicians".	**No direct mention of harm:** 'UMMC has received no notifications from current or former patients regarding any unauthorized use of protected health or personal information pertaining to this breach.'
TW30	20-Mar-13	US	**Unauthorised access**	**Maladministration:** The electronic medical records provider, Lawrence Melrose Medical Electronic Record of Melrose Massachusetts, experienced a data security incident in which an employee of a medical practice gained unauthorized access to patients' personal information at six different healthcare facilities.	**No direct mention of harm**
TW31	10-Mar-13	US	**Non-secure disposal of paper files**	**Maladministration**: A dumpster full of medical documents was found after a medical practice moved premises.	**No direct mention of harm**
TW32	03-Dec-12	US	**Loss of hardware:**	**Maladministration:** The loss of an unencrypted handheld Palm device in the Continuum Home Infusion unit of the University of Virginia Medical Center has resulted in a data breach of protected health information. More than 1,800 patients or potential patients were affected.	**Potential for financial harm:** they are offering credit-monitoring services to victims.
TW33	02-Dec-12	US	**Theft**	**Maladministration**: A company-owned laptop was stolen from the locked car of an Alere employee. The laptop contained patients' electronic health records, which include data such as: Names; Addresses; Dates of birth; Social Security numbers; and Diagnostic codes. Alere did not indicate whether the information was encrypted or if the laptop was password-protected.	**Potential for financial harm:** they are offering credit-monitoring services to victims.

Incident No.	Date	Location	Abuse Type	Abuse Cause	Harm
TW34	30-Nov-12	US	**Unauthorised retention of data**	**Self-gain:** A former resident physician kept patient lists and notes regarding patients in violation of UAMS' policy after leaving the facility on June 3, 2010. The documents contained patient names, partial addresses, medical record numbers, dates of birth, ages, locations of care, dates of service, diagnoses, medications, surgical and other procedure names, as well as lab results.	**No direct mention of harm** – However because the former EE used patient records in a court case against the former ER, documents were disclosed to 3rd parties and were at risk of being in the public court record.
TW35	06-Oct-12	Zambia	**Theft**	**Third Party:** Thousands of cancer patients' lives were put at risk following the looting of computers that store vital data for them at the Cancer Diseases Hospital, a heist that has shocked medical personnel. Theft of computer equipment included data storage devices.	**Individual distress and provision of suboptimal care:** Operations at the hospital, where 350 patients are daily attended to, have screeched to a halt following the theft.
TW36	27-Sep-12	UK	**Unauthorised disclosure**	**Human error:** A member of the public asked the CPS under the FOIA to provide figures for costs and resources used in the Metropolitan Police's Operation Malone – the generic title given to investigations following a series of demonstrations by students against tuition fees in 2010 and 2011. FOI requester received a spreadsheet containing the names of 299 demonstrators arrested not just through Malone, but also during the disturbances and later under another operation, code-named Brontide - included details of defending solicitors, plus some personal observations, including comment on individual medical issues.	**No direct mention of harm**
TW37	21-Sep-12	US	**Theft**	**Maladministration:** A doctor's unencrypted laptop was stolen while he was traveling abroad in 2010.	**No direct mention of harm:** "Given the lack of patient harm discovered in this investigation, Mass. Eye and Ear was disappointed with the size of the fine, especially since the independent specialty hospital's annual revenue is very small compared to other much larger institutions that have received smaller fines."

Incident No.	Date	Location	Abuse Type	Abuse Cause	Harm
TW38	12-Sep-12	UK	**Loss of paper files**	**Maladministration**: Confidential paperwork about mental health patients – including personal details, medical records and care plans – was found 'blowing around' a city centre street in Sheffield.	**Individual distress and institutional harm**: "A big issue for people receiving treatment for mental health issues is paranoia about how their personal details will be handled - and something like this could make them reluctant to seek help or co-operate with health workers.' (Diminish public trust in mental health profession + individual distress)
TW39 (Also in ICOM11)	12-Jul-12	UK	**Unauthorised disclosure**	**Human error:** At St George's Healthcare NHS Trust in London, a vulnerable individual's sensitive medical details were sent to the wrong address.	**No direct mention of harm**
TW40	21-Jun-12	US	**Theft**	**Self-gain**: Over a 17-month period, Laurie Napper used her position at the hospital to gain access to patients' names, addresses and Medicare numbers to sell their information.	**No direct mention of harm**
TW41	16-May-12	US	**Technical security failure**	**Third Party:** A server at the DTS was breached and personal information on around 780,000 Medicaid recipients, including social security numbers of around 280,000 Utah citizens. Hackers started downloading data from the server.	**Potential for financial harm:** they are offering credit-monitoring services to victims.
TW42	01-May-12	UK	**Unauthorised disclosure**	**Human error**: Ayrshire woman whose records were transferred from her GP surgery without her knowledge. Mary Corbey's records were mistakenly sent to a doctors' practice in Manchester. The error meant she was removed as a patient at her own surgery. Ms Corbey only discovered the mistake when she went to the doctor with symptoms consistent with cervical cancer. She found she had been removed from screening programmes years earlier.	**Individual distress**: emotional and physical.
TW43	25-Apr-12	US	**Unauthorised access**	**Without clinical or legitimate justification**: The South Carolina Department of Health and Human Services (SCDHHS) discovered on April 10 that an employee of the state's Medicaid program had transferred personal information of 228,435 Medicaid beneficiaries to his personal email account.	**No direct mention of harm**

Incident No.	Date	Location	Abuse Type	Abuse Cause	Harm
TW44	24-Apr-12	US	**Theft**	**Third Party:** A man brought in several air force medical records dating from 2003 to 2007 that he found in his estranged wife's closet on April 17.	**No direct mention of harm**
TW45	19-Apr-12	UK	**Theft**	**Third Party:** A system used by Pharmacyrepublic Limited, to record the medication handed out to around 2000 patients, was stolen from one of its premises.	**No direct mention of harm**
TW46	30-Jan-12	UK	**Unauthorised access**	**Without clinical or legitimate justification**: An ex-girlfriend probed her ex-boyfriend's medical records while working at Derriford Hospital.	**Individual distress - emotional, physical and financial harm**: 'The court heard the data protection breach and its aftermath significantly affected Mr Grinyer's mental health, aggravating an existing paranoid personality disorder, causing severe stress, anxiety and a breakdown.' Led to loss of earnings and increased medical costs.
TW47	24-Jan-12	US	**Unauthorised access**	**Self-gain:** An Atlanta, Georgia man was sentenced earlier this month to one year and one month in prison for intentionally accessing a computer of a competing medical practice, and taking personal information of the patients. The individual made this improper access in order to send marketing materials to patients at the other practice.	**Individual distress:** harassed by marketing.
TW48 (Also in G16)	31-Oct-11	UK	**Non-secure disposal of paper files**	**Maladministration**: In February 2011, Warwickshire NHS Trust disposed of records relating to the treatment of 18 patients in a communal waste bin at a residential apartment block. At University Hospitals Coventry in May 2011, a member of the public discovered details relating to a patient's sensitive medical procedures and test results. These were "allegedly found in a bin outside Coventry University Hospital", the ICO said.	**Potential Individual distress**: "The Commissioner has taken into account the fact that a proportion of the personal data in question related to medical conditions and could potentially result in distress being caused to the individuals concerned."
TW49	01-Oct-11	US	**Theft**	**Third Party:** Backup tapes from an electronic health care record were stolen from a data contractor's car containing personal and medical records of military patients and their families.	**No direct mention of harm**

Incident No.	Date	Location	Abuse Type	Abuse Cause	Harm
TW50	22-Aug-11	US	**Technical security failure**	**Maladministration:** Southern California Medical-Legal Consultants, which represents doctors and hospitals seeking payment from patients receiving workers' compensation, put their records on a website that it believed only employees could use.	**Individual distress and potential for financial harm (identity theft**): one victim of the data breach - '"I'm totally disgusted about everything," he said, calling the breach "another kick in the stomach."
TW51	10-Aug-11	UK	**Non-secure disposal of paper files**	**Maladministration:** Highly confidential medical files and records were found dumped in the grounds of an abandoned nursing home in Bradford. Included care plans, detailed health assessments and poignant photos of residents who had lived there until its sudden closure in 2008.	**Harm to institution**: community distressed at cavalier way abandoned site treated and personal data left – diminished trust in NHS.
TW52 (Also in Ti09)	03-Aug-11	Ireland	**Unauthorised disclosure**	**Maladministration**: Irish hospital outsourced transcription to the Philippines of medical records and GP letters. The identities of patients may have been disclosed and not all records were returned back.	**No direct mention of harm**
TW53	19-Apr-11	UK	**Non-secure disposal of paper files**	**Maladministration**: Piles of documents revealing student names, photographs, addresses, telephone numbers, dates of birth, and some files exposing sensitive medical information, were found in bin bags at City College.	**No direct mention of harm**
TW54	17-Mar-11	US	**Loss of hardware:**	**Maladministration**: Nine server drives and thus the data of 2 million customers, employees and health care providers were lost. IBM, which managed the company's IT infrastructure, informed Health Net that it was unable to locate server drives.	**Potential for financial harm:** potential for identity theft.
TW55	04-Jan-11	US	**Non-secure disposal of paper files**	**Maladministration**: 50 boxes of personnel records – with medical information – were found dumped outside Plano library after a company went out of business.	**No direct mention of harm**
TW56	22-Oct-10	US	**Loss of hardware:**	**Maladministration**: Keystone Mercy Health Plan and AmeriHealth Mercy Health Plan lost a computer flash drive containing the names, addresses, and personal health information of 280,000 people.	**Potential financial harm (identity theft):** "What's tragic is that this is a particularly vulnerable group of people," Peel said. "They tend to be vulnerable to identity theft, vulnerable to discrimination." Medicaid recipients are low-income people.

Incident No.	Date	Location	Abuse Type	Abuse Cause	Harm
TW57	22-Oct-10	US	**Non-secure disposal of paper files**	**Maladministration**: Hundreds of folders containing medical records and Social Security Numbers were found at the Norman Recycling Centre. The files appear to be associated with two medical practices in the Norman, Oklahoma area.	**No direct mention of harm**
TW58	16-Oct-10	US	**Theft**	**Third Party:** UC Davis Medical Centre officials said financial documents and other data containing information about 900 patients were stolen in an August burglary of a West Sacramento courier service.	**Potential financial harm:** potential for identity theft.
TW59	07-Jul-10	US	**Loss of hardware:**	**Human error:** In November 2009, Health Net reported the loss of a portable external hard drive that contained seven years of medical and personal data on about 1.5 million members across four states.	**Potential for financial harm (identity theft):** In court, damages awarded in 'Two years of credit monitoring; $1 million of identity theft insurance; and Reimbursement for the costs of security freezes'.
TW60	11-Jun-10	US	**Unauthorised access**	**For self-gain**: A hospital was fined for a radiologist accessing the records of 177 patients with no "clinical reason to do so". The radiologist "lost a baby because she was on drugs and wanted to see records of obstetrics to see what the pregnant mothers did to get help".	**No direct mention of harm**
TW61	11-Jun-10	US	**Unauthorised disclosure**	**Maladministration**: A hospital employee allowed a friend into a restricted area, where the visitor could overhear patients discussing their situation.	**No direct mention of harm**
TW62	11-Jun-10	US	**Unauthorised access**	**Without clinical or legitimate justification:** One of the seven people who accessed the record of the patient did so because "she used to know the patient", thus without legitimate basis.	**No direct mention of harm**
TW63	11-Jun-10	US	**Unauthorised access**	**Without clinical or legitimate justification:** Seventeen security guards accessed the medical records of 33 patients without legitimate reason.	**No direct mention of harm**
TW64	11-Jun-10	US	**Unauthorised access**	**Without clinical or legitimate justification:** Accessed patient information because they were "curious."	**No direct mention of harm**

Incident No.	Date	Location	Abuse Type	Abuse Cause	Harm
TW65	11-Jun-10	US	**Unauthorised disclosure**	**Human error**: Records were sent to a lawyer by accident. A patient sues the hospital. Lawyer representing the patient asked for test results for his case. Hospital sends the results, as well as the results for three other people.	**No direct mention of harm**
TW66	07-Apr-10	US	**Theft**	**Third Party:** Two laptops were stolen containing sensitive health information about more than 5,000 patients in the John Muir hospital system.	**No direct mention of harm**
TW67	04-Feb-10	US	**Theft**	**Third Party:** University of California, San Francisco medical school are in the process of notifying 4,310 patients that some of their personal information may have been exposed after a laptop was stolen from an employee in late November 2009. The information included patients' names, medical record numbers, ages, and clinical information, according to a UCSF statement.	**No direct mention of harm**
TW68	27-Jan-10	US	**Theft**	**Third Party:** BlueCross Blue Shield Insurance company had 57 hard drives stolen from their training facility. The hard drives contained audio and video files with identifying information for up to 500,000 members.	**Potential for financial harm:** they are offering credit-monitoring services to victims.
TW69	03-Nov-09	US	**Technical security failure**	**Third Party:** A computer server storing data for a state mammography registry had been "targeted in a computer hack". When the staff discovered the breach, all data on the server was removed. The Registry collected data from participating mammography practices to advance knowledge about the most effective ways to improve breast cancer detection, understand risk factors, guide future research and inform policy makers. Post-breach the individual discovered that not only were her mammography records sent to a registry she didn't even know existed, but that her records may have been hacked.	**Individual distress**: individual distressed by collection of data without her consent or knowledge. Individual distressed by lack of explanation for why certain data were collected and/or relevant to alleged 'purpose' - 'How do my Social Security and phone numbers factor into "their ability to detect cancer"? "Do even Social Security numbers have a greater chance of being diagnosed?" "Does an out-of-state phone number increase the benefit of early detection?" (Quotes from victim)

Incident No.	Date	Location	Abuse Type	Abuse Cause	Harm
TW70	18-Feb-09	US	**Technical security failure**	**Third Party:** Someone illegally gained access to 17 computer servers at the University of Alabama in November 2008. Info breached include lab data: names, addresses, birthdates and Social Security numbers of each person who has had lab work, such as a blood or urine test, done on the UA campus since 1994.	**Potential financial harm:** potential for identity theft.

Table 25: Soft newspaper evidence incidents

	Article	Date	Source	M	Where	Incident
news1.	Mi01	140303	Inquest		Bristol Royal Hospital	Six-month delay in treating Samuel Starr (chronic heart disease). Unclear if timely treatment would have changed outcome (death).
news2.	Mi02	140301	Sunday People, report		Bristol Royal Hospital	Hospital failed to declare death of Luke Jenkins, possibly to provide better figures for National Institute for Cardiovascular Outcomes Research's league tables. Sir Bruce Keough ordered lawyer-lead inquiry into Ward 32.
news3.	Te09	140123	NAO		NHS England Leeds, Oxford, Colchester, North West London Hospitals Trust, Barnet & Chase Farm Hospitals)	Falsifying waiting times (26% of cases) or keeping incomplete records (31%). Only 43% of cases were data properly recorded. Thousands of patients forced to endure long waits because of errors and manipulation of data.
news4.	W01	131119	Health and Professions Council		Welsh Ambulance Service	2 paramedics struck off. 1 failed to properly assess patient, who died. Both fabricated data after death. (Victim, 30 yr. old Sarah Thomas – The Telegraph)
news5.	Te10 G06 Te11 B02	131114 131109 131106 131105	Inquest/ Monitor (Trust Watchdog)		Colchester Uni Hosp	**Te10** and inquest. Woman died after childbirth. Month before baby skull crushed by excessive use of forceps. Special measures for falsifying data. Staff bullied. Police considering whether to launch investigation. **G06** Cancer records falsified to meet national cancer targets; *'Initially that the records of the 22 patients appeared to have been changed ... However, sources close to the investigation now say that 6,000 or more patients referred to the Essex hospital between 2010 and 2013 may be caught up in the scandal'*. **Te11** Fiddling cancer waiting lists. Clerical staff had raised concerns with managers *that 'lives could be jeopardised'*. **B02** Of 61 cases reviewed, 22 showed people had been placed at risk of receiving care that was unsafe or not effective. Hospital bosses failed to investigate allegations. Trust written to 30 patients or next of kin offering to review treatment.
news6.	W02	131004	ICO		Cardiff & Vale	Consultant Psychiatrist looses data not securely fastened to bike's child seat. Included a patient's mental health tribunal report. ICO's findings also showed that while the member of staff concerned could have accessed the file network remotely, thereby negating the need to take the information off-site, insufficient steps had been taken to make employees aware of that fact.

	Article	Date	Source	M	Where	Incident
news7.	Ti04 Ti06 Ti10 Ti14	130901 130120 110612 091227	Health Service Executive		Ireland	**Ti04** Ireland. 18,000 envelopes (est. 80,000 people) received by HSE requesting Guthrie cards to be retained or returned, Supported by SADS Ireland. (Sudden Arrhythmia Death Syndrome or Sudden Adult Death Syndrome). **Ti06** HSE (Ireland) to destroy over 1m blood samples. Doctors oppose this. Dept of Health did not take plea of SADS group into account. Samples used to identify criminals, but also badly burnt victims. **Ti10** Irish families who are victims of SADS urge do not destroy samples on Guthrie cards **G07** Irish hospital has kept children's DNA since 1984. Guthrie cards. To date (2009) 1,548,300 samples. Anonymity but no consent.
news8.	G07	130819	ICO		NHS Surrey	Failed to check that the data destruction company had destroyed records properly. ICO: '*one of worst data breaches ever seen*': Approx. 3000 patients
news9.	B03	130621	ICO		CQC and Furness General Hospital,	Senior CQC members in cover-up at Furness General Hospital where 16 babies died. May constitute a broader cover-up at CQC. Names of individuals originally redacted due to DPA – hiding behind legislation? Jeremy Hunt and ICO intervened due to 'overriding public interest'.
news10.	B04	130426	Public contacted Trust		NI Western Trust	Records in bin bag thrown into lady's garden. 17 Older patients, 6 with DNR. Breach reported to ICO
news11.	S01	130331	ICO		Royal Oldham Hospital	16 Children's' notes on street found by member of the public in the street. Guardians informed
news12.	B05	130215	ICO		NMC/ Cardiff	NMC fined. 3 DVDs for court hearing related to offenses committed by nurse. 'Highly sensitive' info and evidence from vulnerable children. Contract worker to package and courier to a hearing. On arrival DVDs not in package, not encrypted, not found.
news13.	In04	120930	Imperial College Healthcare NHS Trust		Imperial College	Lost medical records for thousands of patients awaiting cancer test results. Serious computer problem + staff mistakes played havoc with waiting lists. 2,500 forced to wait longer than target, further unknown whether 3,000 suspected cases had received tests. Includes 74 cases where patient died. Took five months to inform GPs. 73 died, but Trust claimed that no one died waiting for results or care. Fined by NHS North West London. External review Terry Hanafin, '*serious management failure*'.
news14.	In05	120908	WA member asked to investigate by constituent		Wales and probably elsewhere	Medical records sent to DWP and ATOS opened routinely by Royal Mail staff, to pre-sort (if not marked private and confidential). Came to light after constituent asked WA member to investigate.
news15.	G10	120806	ICO		Torbay Care Trust	Non-clinical data of 1,000+ NHS staff, but sexual orientation name, DOB, NI number. Reported by public. Spreadsheet viewed est. 300 times.
news16.	B08 B07	120721 120720	Belfast Telegraph		Northern Trust, Caseway Hospital	**B08** Batch of 8 patient letters emailed to wrong person, handed over to the Belfast Telegraph. Trust did not immediately inform patient. **B07** Received as a reply to her email regarding her mother's health.
news17.	H02	120622	FoI – Scottish LibDems		Scotland	104 cases of records were reported missing or stolen by NHS boards in Scotland last year. It follows the discovery last week of confidential patient notes dumped beside a bin in Dundee.

	Article	Date	Source	M	Where	Incident
news18.	B09 E10 In06 Ma12	120601 120601 120601 120601	ICO		Brighton & Sussex	**B09** Sub-contractor did not decommission hard drives. Sold on eBay, inc HIV details. No charges brought against him. Sub-contractor removed 252+ hard drives, 232 offered on eBay. **E10** ditto **In6** ditto **Ma12** ditto
news19.	W03	120430	ICO		Aneurin Bevan HB	Consultant mailed letter to secretary, not enough info to identify patient correctly, and patient's name was misspelt. Report therefore sent to wrong patient.
news20.	In09 G28 Ti08	120420 120413 120311	BPAS reported to police		BPAS	**In09** Hacker James Jeffery stole 10,000 records from BPAS (British Pregnancy Advisory Service) website. Jailed for 2yrs 8mths. BPAS – health records were never at risk. However, since arrest 2,500 attempts to hack in, in third cases from North America and from Russia. **G28** Jeffery member of hacking collective *Anonymous*. **Ti08** ditto
news21.	S03	120415	NHS sources		GE Healthcare - USA	NHS technology supplier, GE Healthcare, sent 600,000 records to USA by mistake. Took one year to report incident.
news22.	W04	120228	ICO		Greenbanks Homecare, Cardiff	Details found in alley. Echo newspaper went to check and found more. Why? Greenbanks care home had moved, Alzheimer's Society was sending mail to the old address.
news23.	S04	120215	NHS Tayside/NMC		Royal Victoria, Dundee	Nurse reads 10 records including friends', sacked, stuck off
news24.	S05	111126	Victim approached NHS Lothian		Edinburgh Royal	Cleaner allegedly obtained patient details from PC – but hospital spokesperson maintained information was on floor plan screen about A&E.
news25.	G12 G13 G14	111113 111110 111109	FoI - Guardian Healthcare Network Snapshot Survey		25 biggest Trusts in England	**G12** Survey: 72 actions across 16 Trusts. Increase in staff requesting social media guidance. **G13** Of the 25 Trusts approached, 16 replied. FoI question: How many staff received warnings/dismissed for improper use of social media over last three years. Figures for 2008-2009 and October 2011 were compared. **G14** Lists actions by Trust
news26.	G16	111027	ICO		UH Coventry & Warwickshire	Lost records twice. 18 records in bin in residential area, details of medical procedure in bin outside hospital
news27.	Mi05 In10	111005 111004	ICO		Dartford & Gravesham	**Mi15** Paper records stored in wrong room, destroyed in error, undiscovered for 3 months **In10** 10,000 archived records destroyed by mistake. Put in disposal area b/c lack of space. Apparently no clinical risks
news28.	S06	110924	?		Scottish Government	Scottish Government sent Inpatient Patient Experience survey to 903 dead patients.
news29.	In11	110917	ICO		Eastern & Coastal Kent PCT.	CD sent to landfill site in filing cabinet, 1.6 million at risk. Filing cabinet not recovered.

	Article	Date	Source	M	Where	Incident
news30.	Ti09	110731	DPC		Tallaght Hospital, Ireland	Personal medical records sent to Philippines for transcription. Including report from Consultant Psychiatrist, information probably to go to the Residential Institutions Redress Board which offers compensation to those who were abused in state care.
news31.	S07	110615	ICO		London Health Programmes	Unencrypted laptop missing, took 3 weeks to report to police. Records of 8.63ml people. One of 20 laptops lost or stolen, 8 now recovered.
news32.	B13 Ma10	110218 120718	ICO		Moorgate Primary Care Centre	**B13** Nurse gave patient details to boyfriend (Personal Injury firm). Sacked. Pending court hearing stabbed daughter, unsuccessful suicide attempt, jailed 12 years. Perpetrator was in a *'spiral of descent into despair'* leading up to the killing, a court heard. **Ma10** ditto
news33.	S08	110115	Public		Ross Hall & Nuffield Health Hospitals, Glasgow	Paper and Dictaphone tape found in bin. Apparently sent recorded delivery to employee, incorrectly delivered.
news34.	Ti13	100110	DPC		Children's University Hospital Ireland	2 data servers stolen, potentially 1m patients' data at risk. Happened in 2007, the organisation saw no need to inform public.
news35.	G23	091115	Coroner		Holloway prison	Prisoner's record falsified by nurse (suspended) after suicide; psychopharmaca not administered. Able to enter into EMIS system, but electronic audit revealed that no medication was issued on that day. Inquiry open. Prison governor ordered investigation into incident and potential abuse of EMIS.
news36.	Mi11	091115	ICO		Maidstone & Tunbridge Wells	3 stolen laptops in one month in Kent
news37.	Ma26	091018	ICO		London Clinic (Harley Street) in particular, others also targeted	Data from private hospitals sold illegally to **undercover investigators** - apparently, from men with access to IT companies in India, purportedly records from 'transcription' company. 100 records bought and all authentic. NHS records were included. ICO now investigating. London Clinic did not send material abroad, but had used IT company DGL Information Technologies UK to turn paper into e-records. DGL in turn had contract with Scanning And Data Solutions, who provide scanning service. SAD had further subcontracts, including one with Pune in India.
news38.	S14	090507	None			BT led 5-country academic study with the University of Glamorgan**.** 300 hard-drives were bought at auction. One third had sensitive details, including NHS patient notes.
news39.	E18	090403	Public		Southern General in Glasgow.	Paper records stored in hospital corridor due to lack of space. Found by public, sent photo to Scottish Labour Party.
news40.	S15	090116	?		St Mary's, Imperial College Health Care Trust	Unencrypted laptop stolen. Taken from locked office. 14,000 patients records
news41.	Ti2	140102	FoI - Scottish LibDems	M	Scotland	806 breaches in Scotland in 2009-2013. Greater Glasgow & Clyde, folder with 60 patients' info at a bus stop. Patient letters found in hospital grounds.
news42.	E02 E09	130813 120806	ICO	M	Brighton & Sussex	**E02** Brighton & Sussex data (patients and staff) on hard drives sold online, incl. 1500 HIV positive individuals **E09** ditto

	Article	Date	Source	M	Where	Incident
news43.	E06	130214	FoI – Scottish Conservatives	M	NHS Scotland	Internet misuse: blogs, Flickr, Facebook friends, and sex with patient contacted thru Facebook. 481 misuses since 2010. 30,000 nurses/midwives thought to use social media sites. However, incidence rates include swearing in emails.
news44.	S02	121223	DOH	M	9 NHS trusts, St Leonard's Hospital	Random breaches reported to DOH. How many affected is dealt with locally. Disk with 160,000 children's records failed to arrive at St Leonard's hospital. No evidence of data in wrong hands
news45.	B08	120719	FoI - ?	M	the Five NI Trusts	Breakdown of breaches 2008 to date. Including contact details for domestic violence victim given to violent ex-partner by social worker by mistake; message left on wrong answer-phone; notes left on car roof and car drives away; incorrect email recipient; records left in shop; snooping relative's blood test results
news46.	In07	120514	FoI – Channel 4 Dispatches	M	UK	DWP, staff disciplined for unauthorised disclosure. Breaches by DWP. Only 11 'serious cases', but 4.57 cases daily. DOH does not collect details for all cases of unlawful access
news47.	B11 E13 G15 Ma15 Te19	111028 111028 111028 111028 111028	FoI – Big Brother Watch	M	NHS Trusts England	**B11** July 2008-July 2011: 152 Trusts, at least 806 breaches. 5+ weekly. Social networking sites and inappropriately accessed med info of colleagues or family. **E13** ditto **G15** 23 Social media; 129 details of colleagues/Family; 57 stolen or lost. Request sent to 428 Trusts (UK wide), 354 replies, 55 partial only, 74 not replying **Ma15** 802 incidents led to 102 sackings. **Te19** ditto
news48.	G18 G19 G20	110504 110504 110504	FoI – Guardian Healthcare	M	71 London NHS organisations	**G18** 30 Trusts responded. 899 breaches, a fifth by NHS Barnet. Various breaches inc. Memory stick, fax to wrong person, patient notes in bin, laptop theft (unencrypted). **G19** List of 2008-2011 breaches **G20** Health service staff mainly responsible for breaches, not IT or management. Losing devices or info / inappropriate disposal / giving out data in error**.**
news49.	Ti12	100523	FoI – Sunday Times	M	British hospitals	Secret blood database babies. UK since 1984. Examples Central Manchester UHT, Cambridge UHT, Great Ormond St, Alder Hey. Police and coroners can apply for access.
news50.	S10 Ma23	100425 100405	?	M	NHS London	**S10** 7 Trusts in London send patient data to India for processing. Fear of jigsaw attacks. **Ma23** Data processing to be done in India. Despite pledge from DOH that no personal information would be sent overseas.
news51.	Ma22 G26 G08	100422 061102 130801	Y	M	Unclear	**Ma22** Assorted cases plus Helen Wilkinson. Labelled alcoholic, former NHS manager. Error in coding. 2 year battle to amend record. Went on to form organisation The Big Opt Out. **G26** Included this pre-2009 article, because relevant. **G08** Follow-up article
news52.	Ti15	090208	ICO	M	Inc Hospital Wembley	ICO report, 2 computers stolen from hospital, 400 patients

	Article	Date	Source	M	Where	Incident
news53.	G01 G02 Te04	140225 140224 140224	Health Select Committee Exclude-not breach	x	HSCIC/NHS IT	**G01 and G02** 47m patient records were sold for £2,200 to Staple Inn Actuarial Society. Allegedly data used not for individual case assessment, but to examine the costs of critical illness. HSCIC is unable to provide information dating back to its predecessor, NHS IT. Financial impact: Higher premiums for <50s for critical illness cover. **Te04** HSCIC admits data should not have been sold by its predecessor.
news54.	B10 E11 In08	120425 120425 120425	FiO – ViaSat Exclude – summary could be double	X M	Inc. Midlothian Council	**B10** breakdown of breaches. 730 breaches, of which 178 NHS, 166 LA. 281 human error, 170 hardware/data stolen, 108 lost. 433 cases still to be decided. Private firms worst offenders. These figures from ICO include private firms. **E11** ditto **In08** ditto
news55.	Ma18	110909	exclude USA	x	USA	Data on commercial website for nearly a year until breach discovered. Stanford Hospital. 20,000 patients' emergency details.
news56.	In13	110701	ICO Exclude – position statement	x	NHS England	ICO says culture change needed. Criticises use of laptops, memory sticks etc. Five named HBs agreed to improve.
news57.	G21	110420	FoI – ViaSat Exclude position statement	x	ICO	80% punishments are in the public sector, yet 59% of breaches are in the private sector. Too little punishment outside of public sector. List of breaches by sector
news58.	B14	090809	Question posed by DUP MLA	x	NI	Figures released by NI Health Minister. Nearly 100 medical records lost in 3 years. 8 cases of data breach in 5 year period
news59.	E15 Mi13 B15 E16 G24 In17 Ma27 S13 Mi12	090526 090526 090525 090525 090525 090525 090525 090525 090329	ICO Exclude - summary	x	NHS England Preston Prison Camden Primary Care Trust, Pancras Hospital	**E15** 140 breaches. ICO action in 14 cases over last 6 [incorrect] months. GP downloaded 10,000 records onto unsecured laptop, later stolen and never retrieved. Memory stick 6,360 inmates Preston prison. Camden Primary 2,500 records on PC left beside skip near St Pancras hospital. Not recovered. **Mi13** 140 breaches in 4 months. inc. skip and memory stick **B15** Breakdown of incidence rates of breach. Memory stick encrypted, but password on post-it on the stick. **E16** ditto **G24** Also Cambridge University Hospital memory stick, 741 patients. Found by car wash worker **In17** Also 2,300 cancer patient unencrypted medical records, theft of desktop PC and laptop, Hull & East Yorkshire Hospitals NHS Trust. 2 laptops stolen from Central Middlesex hospital, desktop PC for Northwick Park Hospital after card security system disabled for maintenance. 361 patients' test results lost. **Ma27** ditto **S13** ditto **M12** ditto

	Article	Date	Source	M	Where	Incident
news60.	Ma05	130502				**Mary Kersewll**, former biomedical scientist, asked by Biggleswade Health Centre in Bedfordshire to undertake urine test for kidney conditions she did not have. Paid for copy of her patient notes, not at surgery when she arrived, altercation and her arrest by police. Wrongly recorded – chronic kidney disease, heave smoker, living with Alzheimer's, had had a hysterectomy and double hip replacement.

Table 26: Impact statements from newspaper articles

	Patient/next-of-kin (10 statements)	Citizens' Voice (6 statements)
Data loss and falsification/fabrication		
news1/In04 Imperial College and lost medical records for thousands of patients awaiting cancer test results.		**Patients Association** 'this is unacceptable … especially patients awaiting cancer results, where every day counts. … It's unfair on the patients to have this stress and worry, and the trust should not have tried to hide the fact that they had lost these records'.
Falsification/fabrication		
news9/B03 CQC and Furness General Hospital cover-up	**Bereaved father** James Titcombe: '"We repeatedly asked why he didn't need antibiotics and were reassured that he seemed fine and there was no reason to give them to him." …He has led the campaign for a public inquiry into "serious systemic failures" … and called reports of a cover-up at the Care Quality Commission "shocking. …"It embodies everything wrong with the culture in the NHS."'	
news5/Te11 Colchester University Hospital, where cancer records were falsified to meet national cancer targets	The **widow of one patient** who 'died of cancer last year …, after being denied vital scans and treatment for months, said she was left "crying down the phone" to medical staff, pleading for them to treat her husband.' 'The **mother of a four-year-old boy** who died of a brain tumour last year, after delays in treatment at the hospital … called for "justice" for her son, and said no-one at the NHS trust had been held accountable for the failings, or even disciplined.'	**Patients' Association**, 'The target-driven culture and the fact that senior people in charge of our patients are prepared to falsify patients is deeply worrying. …There is a question of morality here. Dishonesty at this level is so serious and those responsible must be held to account.'
news3/Te09 NHS England Leeds, Oxford, Colchester, North West London Hospitals Trust, Barnet & Chase Farm Hospitals) falsifying waiting times		**Patients Association** 'It's scandalous that hospitals have been able to get away with this. NHS trusts have been able to manipulate the figures … [which] means that we have no idea how many patients have been forced to wait far too long, increasing the risks to their health.'
news2/Mi02 Bristol Royal Hospital failed to declare death of Luke Jenkins	Parents believe Trust chiefs 'covered up deaths and blatantly lied'.	
Human error		
news51/Ma22 Patient incorrectly labelled alcoholic in GP surgery records	'I went ballistic. To be labelled an alcoholic – who had seen it? Who knows, literally hundreds could have seen it.'	

	Patient/next-of-kin (10 statements)	Citizens' Voice (6 statements)
Ma05 Patient found major errors in GP patient record. Had requested these, not available as agreed, arrested by police	'I was utterly shocked … it read like a post-mortem, it really did. … It could have been really dangerous. Who knows what implications these errors could have had if I'd been taken to hospital in an emergency?'	
news19/W03 Aneurin Bevan Health Board, where consultant mailed letter to secretary and report therefore sent to wrong patient.		**Big Brother Watch:** 'It is incredible the Information Commissioner's Office still requires permission from individual NHS bodies to investigate if they are failing to protect patient information. ... The Commissioner should be able to spot-check any organisation to ensure privacy is being taken seriously.'
news28/S06 Scottish Government sent survey to 903 dead patients.		**Scotland Patients Association** 'branded the blunder "outrageous" and said grieving families deserved an apology. … "Someone should take a fall for this because it is absolutely shocking. It is unforgivable and I hope they extend an unreserved apology."'
Unauthorised/inappropriate disclosure		
news37/Ma26 London Clinic (not exclusively), Harley Street, data sold illegally to undercover investigators	**Nick Dawson**, 'But this is our life – this is your flesh and bones you're talking about here. It's just one step up from grave-robbing'	
news24/S05 Edinburgh Royal, cleaner allegedly obtained patient details from PC and harassed her	**Victim** 'I didn't know who he was, what he was capable of. I didn't know if he was just going to turn up at the house. It's just wrong.'	
news16/B08 Northern Trust, Caseway Hospital and patient letters emailed to incorrect recipient	**Patient affected** 'This is a complete shock, I know nothing about it … I did [undergo the test], but nobody knows that. All that I got done, I hid that from my mother. She knows nothing about anything.'	
news14/In05 Wales and probably elsewhere. Medical records sent to DWP and ATOS opened routinely by Royal Mail staff	**John Williams**. 'People are sending very personal information and have a right to know this is happening; I feel like I've been misled.'	
news49/Ti12 British hospitals and Guthrie cards	**Shami Chakrabarti**, (also member of **Liberty)**: '"As someone who gave consent for my own baby to be tested, I'm horrified that anyone would breach my trust, keep my child's sample for years on end and use it for all sorts of extraneous purposes."'	**GeneWatch**: '"Giving mothers a leaflet does not amount to informed consent. No one who has just given birth is in a state to understand the full implications of how their baby's genome might be used in future."'

Table 27: Reference List for newspaper articles

B02	Trust reported over cancer data. (2013, November 5). *The Belfast Telegraph*. Retrieved from http://www.belfasttelegraph.co.uk/news/local-national/uk/trust-reported-over-cancer-data-29728348.html
B03	Cooper, C. (2013, June 21). NHS baby deaths cover-up: Official who said information could never get into public domain identified as media manager still working at Care Quality Commission. *The Belfast Telegraph*. Retrieved from http://www.belfasttelegraph.co.uk/news/health/nhs-baby-deaths-coverup-official-who-said-information-could-never-get-into-public-domain-identified-as-media-manager-still-working-at-care-quality-commission-29361477.html
B04	Deeney, D. (2013, April 26). Medical records from Waterside Hospital found dumped in woman's garden. The Belfast Telegraph. Retrieved from http://www.belfasttelegraph.co.uk/news/local-national/northern-ireland/medical-records-from-waterside-hospital-found-dumped-in-womans-garden-29223040.html
B05	Nursing body fined over lost data. (2013, February 15). *The Belfast Telegraph*. Retrieved from http://www.belfasttelegraph.co.uk/news/local-national/uk/nursing-body-fined-over-lost-data-29074324.html
B06	Rutherford, A. (2012, July 21). Patient's shock after scan results emailed to stranger. *The Belfast Telegraph*. Retrieved from http://www.belfasttelegraph.co.uk/news/local-national/northern-ireland/patients-shock-after-scan-results-emailed-to-stranger-28773186.html
B07	Rutherford, A. (2012, July 21). New patient data blunder as woman is emailed private details of eight other people. *The Belfast Telegraph*. Retrieved from http://www.belfasttelegraph.co.uk/news/local-national/northern-ireland/new-patient-data-blunder-as-woman-is-emailed-private-details-of-eight-other-people-28772736.html
B08	Patient's details on Facebook after call blunder. (2012, July 19). The Belfast Telegraph. Retrieved from http://www.belfasttelegraph.co.uk/news/local-national/northern-ireland/patients-details-on-facebook-after-call-blunder-28772357.html
B09	NHS trust fined over privacy breach. (2012, June 1). *The Belfast Telegraph*. Retrieved from http://www.belfasttelegraph.co.uk/news/local-national/uk/nhs-trust-fined-over-privacy-breach-28756035.html
B10	Six fines issued for data breaches. (2012, April 25). *The Belfast Telegraph.* Retrieved from http://www.belfasttelegraph.co.uk/news/local-national/uk/six-fines-issued-for-data-breaches-28741733.html
B11	NHS patient data 'put on Facebook'. (2011, October 28). *The Belfast Telegraph.* Retrieved under http://www.belfasttelegraph.co.uk/news/local-national/uk/nhs-patient-data-put-on-facebook-28674595.html
B13	Data probe over dead Chloe's mother. (2011, February 8). *The Belfast Telegraph.* Retrieved from http://www.belfasttelegraph.co.uk/news/local-national/uk/data-probe-over-dead-chloes-mother-28590584.html
B14	Smyth, L. (2009, August 9). 100 medical records lost by NHS in three years. *The Belfast Telegraph.* Retrieved from http://www.belfasttelegraph.co.uk/news/local-national/100-medical-records-lost-by-nhs-in-three-years-28442626.html
B15	NHS 'loses' thousands of files. (2009, May 25). *The Belfast Telegraph.* Retrieved from http://www.belfasttelegraph.co.uk/news/local-national/nhs-loses-thousands-of-files-28480357.html
E02	'More firms' breaching data rules. (2013, August 13). *Express*. Retrieved from http://www.express.co.uk/news/uk/339446/More-firms-breaching-data-rules
E06	Herbert, D. (2013, February 14). Alert over NHS net abuse. *Express*. Retrieved from http://www.express.co.uk/news/health/377591/Alert-over-NHS-net-abuse
E09	Health Trust fined over data breach. (2012, August 6). *Express*. Retrieved from http://www.express.co.uk/news/uk/337968/Health-trust-fined-over-data-breach
E10	NHS trust fined over privacy breach. (2012, June 1). *Express*. Retrieved from http://www.express.co.uk/news/uk/323892/NHS-trust-fined-over-privacy-breach
E11	Six fines issued for data breaches. (2012, April 25). *Express.* Retrieved from http://www.express.co.uk/news/uk/316421/Six-fines-issued-for-data-breaches
E13	NHS patient data 'put on Facebook'. (2011, October 28). *Express.* Retrieved under http://www.express.co.uk/news/uk/280211/NHS-patient-data-put-on-Facebook

E15	Clout, L. (2009, May 26). How the NHS is losing private data every day. *Express*. Retrieved from http://www.express.co.uk/news/uk/103400/How-the-NHS-is-losing-private-data-every-day
E16	Thousands of records 'lost' by NHS. (2009, May 25). *Express*. Retrieved from http://www.express.co.uk/news/uk/103281/Thousands-of-records-lost-by-NHS
E17	Duffy, J. (2009, May 8). NHS records found on second-hand PC disks. *Scottish Express.* Retrieved from http://www.express.co.uk/sport/rugbyunion/99760/NHS-records-found-on-second-hand-PC-disks
E18	Gilbride, P. (2009, April 3). Hospital acts after security blunder. *Express*. Retrieved from http://www.express.co.uk/news/uk/92978/Hospital-acts-after-security-blunder
G01	Ramesh, R. (2014, February 25). MPs' anger at missing data on who has patient records. The Guardian. Retrieved from http://www.theguardian.com/global/2014/feb/25/jeremy-hunt-nhs
G02	Quinn, B. (2014, February 24). Hospital records of 47m NHS patients obtained by insurance society. *The Guardian*. Retrieved from http://www.theguardian.com/society/2014/feb/24/hospital-records-nhs-patients-insurance
G06	Taylor, D. (2013, November 9).Colchester hospital hit by fresh fears over falsified cancer records. *The Guardian*. Retrieved from http://www.theguardian.com/society/2013/nov/09/colchester-hospital-falsified-cancer-records
G07	NHS Surrey's £200,000 data breach scandal: what not to do. (2013, August 19). The Guardian. Retrieved from http://www.theguardian.com/media-network/media-network-blog/2013/aug/19/nhs-surrey-data-breach-scandal
G08	Ramesh, R., & Dinsdale, P. (2013, August 1). Patient lost £18,000 legal battle over GP medical records. *The Guardian*. Retrieved from http://www.theguardian.com/politics/2013/aug/01/patient-legal-battle-medical-records
G10	Press Association. (2012, August 6). NHS trust fined £175,000 for 'troubling' data security breach. The Guardian. Retrieved from http://www.theguardian.com/uk/2012/aug/06/nhs-trust-fined-data-security
G12	Laya, S. (2011, November 13). NHS Facebook misuse should be resolved at local level. The Guardian. Retrieved from http://www.theguardian.com/healthcare-network/2011/dec/13/nhs-facebook-misuse-resolved-managers
G13	Laya, S. (2011, November 10). NHS staff aren't stupid. Their misuse of Facebook is. *The Guardian*. Retrieved from http://www.theguardian.com/healthcare-network/2011/nov/10/informatics-communications
G14	Lays, S. (2011, November 9). Trusts reveal abuse of social media. *The Guardian*. Retrieved from http://www.theguardian.com/healthcare-network/2011/nov/09/trusts-reveal-staff-abuse-of-social-media-facebook
G15	Laja, S. (2011, October 28). NHS staff breach personal data 806 times in three years. *The Guardian*. Retrieved from http://www.theguardian.com/healthcare-network/2011/oct/28/nhs-staff-breach-personal-data-806-times
G16	Hitchcock, G. (2011, October 27). ICO censures trust over patient data loss. *The Guardian.* Retrieved from http://www.theguardian.com/healthcare-network/2011/oct/27/ico-university-hospitals-coventry-warwickshire-trust-data-loss
G18	Laja, S. (2011, May 4). NHS Barnet reveals 187 breaches of personal data. *The Guardian*. Retrieved from http://www.theguardian.com/healthcare-network/2011/may/04/nhs-barnet-187-data-breaches-staff
G19	Personal data breaches by London NHS trusts, 2008-11. (2011, May 4). *The Guardian*. Retrieved from http://www.theguardian.com/healthcare-network/2011/may/04/personal-data-breaches-london-nhs-trusts-data
G20	Laja, S. (2011, May 4). The biggest threat to NHS data security: its staff. *The Guardian*. Retrieved from http://www.theguardian.com/healthcare-network/2011/may/04/biggest-threat-nhs-data-security-staff
G21	Halliday, J. (2011, April 20). Technology blog: ICO 'only punished 1% of all data breaches in past year'. *The Guardian*. Retrieved from http://www.theguardian.com/uk/blog/2011/apr/20/ico-fines
G23	Taylor, D. (2009, November 15). Medical records falsified after Holloway prison death. *The Guardian*. Retrieved underhttp://www.theguardian.com/society/2009/nov/15/holloway-prison-medical-records
G24	Lost medical records force urgent security review. (2005, May 25).*The Guardian*. Retrieved from http://www.theguardian.com/society/2009/may/25/medical-records-security-breach
G26	Evans, R. (2006, November 2). The woman falsely labelled alcoholic by the NHS. *The Guardian*. Retrieved from http://www.theguardian.com/society/2006/nov/02/health.epublic

G28	Mailk, S. (2012, April 13). BPAS hacker jailed for 32 months. *The Guardian.* Retrieved from http://www.theguardian.com/world/2012/apr/13/bpas-hacker-james-jeffery-jailed/print
H02	Currie, B. (2012, June 22). Investigation call over loss of patients' records. *The Scottish Herald*. Retrieved from http://www.heraldscotland.com/politics/political-news/investigation-call-over-loss-of-patients-records.17918479
In04	Manning, S. (2012, September 30). NHS 'cover-up' over lost cancer patient records. The Independent. Retrieved from http://www.independent.co.uk/life-style/health-and-families/health-news/nhs-coverup-over-lost-cancer-patient-records-8191066.html?origin=internalSearch
In05	Lakhani, N. (2012, September 8). Royal Mail staff given access to confidential medical details. *The Independent*. Retrieved from http://www.independent.co.uk/news/uk/home-news/royal-mail-staff-given-access-to-confidential-medical-details-8118203.html?origin=internalSearch
In07	Milmo, C. (2012, May 14). Medical and social security records being stored unlawfully and inappropriately accessed, statistics show. *The Independent*. Retrieved from http://www.independent.co.uk/news/uk/home-news/medical-and-social-security-records-being-stored-unlawfully-and-inappropriately-accessed-statistics-show-7743388.html?origin=internalSearch
In08	Johnson, W. (2012, April 25). Six fines issued for data breaches. *The Independent*. Retrieved from http://www.independent.co.uk/news/uk/home-news/six-fines-issued-for-data-breaches-7677935.html?origin=internalSearch
In09	Cassidy, S. (2012, April 20). Campaigners hack into abortion site provider. *The Independent*. Retrieved from http://www.independent.co.uk/life-style/health-and-families/health-news/campaigners-hack-into-abortion-site-provider-7661516.html?origin=internalSearch
In10	Johnson, W. (2011, October, 4). NHS trust destroyed patient records. *The Independent*. Retrieved from http://www.independent.co.uk/life-style/health-and-families/health-news/nhs-trust-destroyed-patient-records-2365407.html?origin=internalSearch
In11	Johnson, W. (2011, September 17). 1.6m patients' records on CD sent to landfill. *The Independent*. Retrieved from http://www.independent.co.uk/life-style/health-and-families/health-news/16m-patients-records-on-cd-sent-to-landfill-2356182.html?origin=internalSearch
In13	Kendall, K. (2011, July 1). NHS records 'culture change' urged. *The Independent*. Retrieved from http://www.independent.co.uk/life-style/health-and-families/health-news/nhs-records-culture-change-urged-2305348.html?origin=internalSearch
In17	Savage, M. (2005, May 25). NHS 'loses' thousands of medical records. *The Independent*. Retrieved from http://www.independent.co.uk/news/uk/politics/nhs-loses-thousands-of-medical-records-1690398.html?origin=internalSearch
In6	Halfpenny, M. (2012, June 1). Brighton and Sussex University Hospitals NHS Trust fined over privacy breach. *The Independent*. Retrieved from http://www.independent.co.uk/life-style/health-and-families/health-news/brighton-and-sussex-university-hospitals-nhs-trust-fined-over-privacy-breach-7811300.html?origin=internalSearch
Ma10	Parveen, N. (2012, July 18). Nurse who stabbed her four-year-old girl to death is jailed for 12 years: Despair of mother sacked for leaking patient details. *The Daily Mail*. Retrieved from http://www.dailymail.co.uk/news/article-2195788/Dawn-Makin-Nurse-stabbed-daughter-Chloe-Burke-4-death-jailed-12-years.html
Ma12	Smith, G. (2012, June 1). NHS trust fined record £325,000 for auctioning off online computer hard drives filled with HIV patients' details. *Daily Mail*. Retrieved from http://www.dailymail.co.uk/health/article-2153285/NHS-trust-fined-record-325-000-auctioning-hard-drives-filled-HIV-patients-details-online.html
Ma15	Borland, S. (2011, October 28). The nurses who gossip about patients on Facebook and how they are spying on their loved ones. *The Daily Mail.* Retrieved from http://www.dailymail.co.uk/news/article-2054436/The-nurses-gossip-patients-Facebook-spying-loved-ones.html
Ma18	Duell, M. (2011, September 9). Privacy breach leaves personal details of 20,000 hospital patients online for a YEAR. *The Daily Mail*. Retrieved from http://www.dailymail.co.uk/news/article-2035556/Stanford-Hospital-privacy-breach-sees-personal-details-20-000-patients-online-year.html
Ma22	Brennan, Z. (2010, April 22). For sale: Your most intimate secrets... thanks to the national NHS database. *The Daily Mail*. Retrieved from http://www.dailymail.co.uk/news/article-1267892/Putting-health-records-national-NHS-database-save-lives-deeply-disturbing-questions-remain.html
Ma23	Martin, D. (2010, April 5). NHS sends confidential patients' records to India despite pledges it would not. *The Daily Mail*. Retrieved from http://www.dailymail.co.uk/news/article-1263526/NHS-sends-confidential-patients-records-India-despite-pledges-not.html

Ma26	Macfarlane, J. (2009, October 18). Private medical records for sale: Harley Street clinic patients' files outsourced for computer input - and end up on black market. *The Daily Mail*. Retrieved from http://www.dailymail.co.uk/news/article-1221186/Private-medical-records-sale-Harley-Street-clinic-patients-files-outsourced-input--end-black-market.html
Ma27	'Cavalier' NHS workers lose tens of thousands of medical records. (2005, May 25). *The Daily Mail*. Retrieved from http://www.dailymail.co.uk/news/article-1187248/Cavalier-NHS-workers-lose-tens-thousands-medical-records.html
Mi01	Pedley, T. (2014, March 3). Three-year-old heart patient died after six-month delay for key appointment 'because of computer glitch'. *Daily Mirror*. Retrieved from http://www.mirror.co.uk/news/uk-news/samuel-starr-death-three-year-old-heart-3204234
Mi02	Boyle, S. (2014, March 1). Officials 'fiddled' death figures at scandal-hit Bristol Royal Hospital for Children. *Daily Mirror*. Retrieved from http://www.mirror.co.uk/news/uk-news/bristol-royal-hospital-children-death-3197538
Mi05	Gregory, A. (2011, October 5). Hospital accidentally destroys medical records of 10,000 patients. *The Daily Mirror*. Retrieved from http://www.mirror.co.uk/news/uk-news/hospital-accidentally-destroys-medical-records-83282
Mi11	Sunday People. (2009, November 15). Three raids on hospital record PCs. The Mirror. Retrieved from http://www.mirror.co.uk/news/world-news/three-raids-on-hospital-record-pcs-1673001
Mi12	NHS patients in PC disaster. (2009, March 29). *The Daily Mirror*. Retrieved from Ehttp://www.mirror.co.uk/news/world-news/nhs-patients-in-pc-disaster-1664260
Mi13	Personal records of patients lost by NHS. (2009, May 26). *The Daily Mirror*. Retrieved from http://www.mirror.co.uk/news/uk-news/personal-records-of-patients-lost-by-nhs-396159
S01	Bradley, C. (2013, March 31). Sick kids' hospital notes left n street. *The Sun*. Retrieved from http://www.thesun.co.uk/sol/homepage/news/article4867155.ece
S02	DoH! We've lost patient data. (2012, December 23). *The Sun*. Retrieved from http://www.thesun.co.uk/sol/homepage/news/615297/DoH-Weve-lost-patient-data.html
S03	Elliott, A. (2012, April 15). NHS files fiasco as 600,000 patients' data sent abroad. *The Sun*. Retrieved from http://www.thesun.co.uk/sol/homepage/news/4257602/NHS-files-fiasco-as-600000-patients-data-sent-abroad.html
S04	Pooran, N. (2012, February 15). Nurse snooped on friends' files. *The Scottish Sun.* Retrieved from http://www.thescottishsun.co.uk/scotsol/homepage/news/4133003/Nurse-snooped-on-friends-files.html
S05	Lavelle, C. (2011, November 26). Cleaner contacts patient on Facebook. *The Scottish Sun*. Retrieved from http://www.thescottishsun.co.uk/scotsol/homepage/news/3961285/Cleaner-contacts-patient-on-Facebook.html
S06	Robson, C. (2011, September 24). NHS survey sent to 900 dead patients. *The Scottish Sun.* Retrieved from http://www.thescottishsun.co.uk/scotsol/homepage/news/3833190/NHS-surveys-sent-to-900-dead-patients.html
S07	Sullivan, M. (2011, June 15). Missing: Laptop with 8.6million medical records*. The Sun.* Retrieved from http://www.thesun.co.uk/sol/homepage/news/3637704/Missing-Laptop-with-86million-medical-records.html
S08	Thornton, P. (2011, January 15). Doc files dumped in a bin. *The Scottish Sun*. Retrieved from http://www.thescottishsun.co.uk/scotsol/homepage/news/3353092/Doc-files-dumped-in-a-bin.html
S10	Morton, E. (2010, April 25). NHS patients' secrets outsourced to India. *The Sun*. Retrieved from http://www.thesun.co.uk/sol/homepage/news/2920489/Millions-of-patient-records-are-being-sent-to-India-by-the-NHS.html
S13	Medical records lost by NHS. (205, May 25). *The Sun*. Retrieved from http://www.thesun.co.uk/sol/homepage/news/2447240/Medical-records-lost-by-NHS.html
S14	Crime is easy PC. (2009, May 7). *The Sun*. Retrieved from http://www.thesun.co.uk/sol/homepage/news/2417903/Crime-is-easy-PC.html
S15	NHS patient files on stolen PC. (2009, January 16). *The Sun*. Retrieved from http://www.thesun.co.uk/sol/homepage/news/2142440/Patient-details-on-laptop-stolen-from-NHS-hospital.html
Te04	Donnelly, L. (2013, September 1). Patient records should not have been sold, NHS admits. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/health/nhs/10659147/Patient-records-should-not-have-been-sold-NHS-admits.html

Te09	Donnelley, L. (2014, January 23). One in four hospitals records false waiting times. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/health/healthnews/10590713/One-in-four-hospitals-records-false-waiting-times.html
Te10	Donnelley, L. & agencies. (2013, November 14). Scandal cancer trust placed in special measures. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/news/uknews/10450684/Scandal-cancer-trust-placed-in-special-measures.html
Te11	Donnelley, L., & Dixon, H. (2013, November 6). Hospital was warned about cancer waiting list fiddling two years ago. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/journalists/laura-donnelly/10431470/Hospital-was-warned-about-cancer-waiting-list-fiddling-two-years-ago.html
Te19	Rainey, S. (2011, October 28). Nurses discuss ill patients on Facebook, study finds. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/health/healthnews/8854658/Nurses-discuss-ill-patients-on-Facebook-study-finds.html
Ti02	Scotland Staff. (2014, January 2). Patient health records lost. *The Times*. Retrieved from http://www.thetimes.co.uk/tto/news/article3963337.ece
Ti04	Tighe, M. (2013, September 1). 80,000 want to save their blood samples. *The Sunday Times*. Retrieved from http://www.thesundaytimes.co.uk/sto/news/ireland/article1307685.ece
Ti06	Tighe, M. (2013, January 20). Doctors oppose destruction of 'priceless' baby blood samples. *The Sunday Times*. Retrieved from http://www.thesundaytimes.co.uk/sto/news/ireland/article1198068.ece
Ti08	Henry, R. (2012, March 11). Hacker steals patient records. The Sunday Times. Retrieved from http://www.thesundaytimes.co.uk/sto/news/uk_news/Tech/article991553.ece
Ti09	Mooney, J. (2011, July 31). New probe on medical leak. *The Sunday Times.* Retrieved from http://www.thesundaytimes.co.uk/sto/news/ireland/News/Irish_News/article681924.ece
Ti10	Tighe, M. (2011, June 12). Health minister urged not to destroy 1m 'vital' blood samples. *The Sunday Times*. Retrieved from http://www.thesundaytimes.co.uk/sto/news/ireland/article646749.ece
Ti12	Woolf, M. (2010, May 23). NHS uses babies' blood for secret DNA database. *The Sunday Times*. Retrieved from http://www.thesundaytimes.co.uk/sto/news/uk_news/Health/article297353.ece
Ti13	Tighe, M. (2010, January 10). Records stolen from hospital that held secret DNA database. *The Sunday Times*. Retrieved from http://www.thesundaytimes.co.uk/sto/news/world_news/article194714.ece
Ti14	Tighe, M. (2009, December 27). Hospital keeps secret DNA file*. The Sunday Times*. Retrieved from http://www.thesundaytimes.co.uk/sto/news/world_news/article193912.ece
Ti15	Mostrous, A. (2009, February 8). UK citizens' private information being lost at record rate. *The Times*. Retrieved from http://www.thetimes.co.uk/tto/news/politics/article2026898.ece
W01	Paramedics struck off for falsifying patient data. (2013, November 19). *The Western Mail/WalesOnline*. Retrieved from http://www.walesonline.co.uk/news/wales-news/paramedics-struck-falsifying-patient-data-6320550
W02	Bevan, N. (2013, October 4). Health board criticised after consultant's patient notes go missing on a bike ride home. *Western Mail/WalesOnline*. Retrieved from http://www.walesonline.co.uk/news/health/health-board-criticised-after-consultants-6135401
W03	Health board fined for "serious breach" of Data Protection Act. (2012, April 30). *Western Mail/WalesOnline*. Retrieved from http://www.walesonline.co.uk/news/wales-news/health-board-fined-serious-breach-2049161
W04	Care home patients' confidential details found in alley. (2012, February 28). *Western Mail/WalesOnline*. Retrieved from http://www.walesonline.co.uk/news/local-news/care-home-patients-confidential-details-2043410

Table 28: Journals, trade magazines and blogs future research search

Journals

Website and search terms	Hits	Relevant	Comment
BMJ Website			
"data AND protection AND health"	12779	-	* = truncated after 300
"harm AND health AND data"	12384	-	
"health AND data"	8802	-	
"biomedical AND data"	281	-	
"genetic AND data"	633	-	
"patient AND record"	3597	-	
"patient AND data"	9028	-	
"patient AND abuse"	1534	-	
Total	**49038**	**-**	
Journal of Health Organisation and Management			
"data AND protection AND health"	55	0	
"harm AND health AND data"	45	0	
"health AND data"	381	0	
"biomedical AND data"	28	0	
Total	**509**	**0**	
BMJ News			
"data AND protection AND health"	301	6	
"harm AND health AND data"	207	0	
"health AND data"	3043	0*	
"biomedical AND data"	144	2	
"genetic AND data"	152	0	
"health AND record"	1257	0*	
"patient AND record"	992	0*	
"abuse AND patient"	430	3*	
Total	**6526**	**11**	
BMJ Comment			
"data AND protection AND health"	462	1*	
"harm AND health AND data"	985	0*	
"biomedical and data"	411	0*	
"genetic AND data"	509	0*	
"health AND record"	2077	1*	
"patient AND record"	2013	0*	
"abuse AND patient"	718	0*	
Total	**7175**	**2**	

Trade Magazines

Website and search terms	Hits	Relevant	Comment
Computer Weekly			
"health AND data AND harm"	97	1	
"health AND data"	100	0	
"biomedical AND data"	89	0	
"genetic AND data"	100	0	

"health AND record"	100	0	
"patient AND record"	100	2	
"patient AND abuse"	87	0	
Total	**673**	**3**	
SC Magazine			
"health AND data AND harm"	6	3	
"health AND data"	161	28†	† = truncated after 40
"biomedical AND data"	2	0	
"genetic AND data"	1	0	
"health AND record"	29	20	
"patient AND record"	16	15	
"patient AND abuse"	1	0	
Total	**216**	**66**	
Professional Security			
"health AND data AND harm"	62	1	
"health AND data"	229	8††	† = truncated after 280
"biomedical AND data"	0	0	
"genetic AND data"	9	0	
"health AND record"	51	0	
"patient AND record"	126	7	
"patient AND abuse"	51	0	
"health AND record"	601	7†††	† = truncated after 300
Total	**1129**	**23**	

Blogs

Website and search terms	**Hits**	**Relevant**	**Comment**
Privacy International			
"harm AND health AND data"	3	0	
"health AND data"	28	0	
"biomedical AND data"	0	0	
"genetic AND data"	6	0	
"health AND record"	5	0	
"patient AND record"	1	0	
"abuse AND patient"	1	0	
Total	**44**	**0**	
Science and Society (Duke)			
"harm AND health AND data"	1	0	
"health AND data"	4	0	
"biomedical AND data"	0	0	
"genetic AND data"	7	0	
"health AND record"	5	0	
"patient AND record"	2	0	
"abuse AND patient"	1	0	
Total	**20**	**0**	

Datonomy			
"harm AND health AND data"	5	0	
"health AND data"	30	2	
"biomedical AND data"	1	0	
"genetic AND data"	3	0	
"health AND record"	8	0	
"patient AND record"	5	0	
"abuse AND patient"	0	0	
Total	**52**	**2**	
BTO Solicitors			
"harm AND health AND data"	1	0	
"health AND data"	8	0	
"biomedical AND data"	0	0	
"genetic AND data"	0	0	
"health AND record"	13	0	
"patient AND record"	0	0	
"abuse AND patient"	0	0	
Total	**22**	**0**	
Field Fisher Privacy and Information Law			
"harm AND health AND data"	0	0	
"health AND data"	12	0	
"biomedical AND data"	0	0	
"genetic AND data"	0	0	
"health AND record"	5	0	
"patient AND record"	2	0	
"abuse AND patient"	0	0	
Total	**19**	**0**	
Hogan Lovells Chronicle of Data Protection			
"harm AND health AND data"	24	0	
"health AND data"	124	7	
"biomedical AND data"	0	0	
"genetic AND data"	6	0	
"health AND record"	38	5	
"patient AND record"	15	3	
"abuse AND patient"	1	0	
Total	**208**	**15**	
Pogowasright			
"harm AND health AND data"	19	2	
"biomedical AND data"	1	0	
"genetic AND data"	24	0	
"health AND record"	135	7	
"patient AND record"	38	7	
"abuse AND patient"	6	0	
"health AND data"	203	17	
Total	**426**	**33**	