Nuffield Council's consultation on Biological and Health Data

The following is the response of the Northern Ireland (NI) Privacy Advisory Committee[1] (PAC) to the Nuffield Council's consultation on Biological and Health Data.

Overview

This is an important consultation on the ethical challenges in relation to proposed uses and disclosure of person and typically patient derived biomedical information. We begin by suggesting that consideration of the questions posed in this consultation should be prefaced by an appreciation of the pivotal importance of patient confidentiality and informational privacy in the context of health and health care. It is on these matters that we feel best able to provide comment.

First, a major source of the requirement of patient confidentiality is the fact that the relationship between the healthcare professional and the patient is one of 'fidelity' or 'trust'. Within the relationship between the healthcare professional and the patient, there exists a tacit understanding on the part of the patient that confidential information (ie personal identifiable information) will not be further used or disclosed without the awareness and consent of the patient.

Second is the right to privacy. The right to respect for private life is a well-established right in the European tradition. This right guarantees the protection of the person against the intervention or interference of public authorities in the private sphere and it embraces, but is not restricted to, the protection of personal information.

Third is the right to self-determination. Just as a patient has a right to self-determination in various other health care matters, it ought normally to be that patient's decision as to who should have access to their personal identifiable health information and the purpose for which it may be used.

A fourth reason for respecting confidences in health care is that doing so enables patients to disclose sensitive information that health staff need to provide treatment or care. Without an assurance that confidentiality will be maintained, patients might be less willing to disclose information, resulting in obstacles to their effective care and negative effects for their health and for public health.

Together these arguments provide a strong ethical case for the non-use or non-disclosure of person identifiable biomedical information, outside direct care provision, in the absence of express consent.

That said none of the arguments stated above lead to the conclusion that the ethical duty of confidentiality is absolute. However where the proposed use or disclosure of patient identifiable information is not directly for their care, the express consent of that service user is usually required. The possible exceptions to this requirement for consent are where a statute, court or tribunal imposes a requirement to disclose or there is an *over-riding* public interest in the use or disclosure.

Many uses of service user information are increasingly required for evidence-based healthcare practice and for a rational approach to service provision. The following are examples of such secondary uses: planning; financial management; commissioning of services; investigating complaints; auditing accounts; teaching; health and health care research; public health monitoring; registries; infectious disease reporting. Key to such secondary uses is assuring that patient derived

data is only accessible in an unidentifiable (de-identified) form and that patients cannot subsequently be re-identified.

Consultation Questions

1. Do biomedical data have a special significance?

In relation to confidentiality biomedical data is among the most sensitive. They belong to a person's private sphere along with other personal and sensitive information.

Genomic data sets present challenges, although not unique, relating to potential future benefits to the individual and others, including close relatives. In relation to the core principles informing privacy and confidentiality (considered above) processes and procedures for obtaining consent and re-consenting are required. Relevant functions including data linkage and re-contacting of individuals at some future date by those with a direct care relationship can often be achieved through the services of appropriately regulated Honest Broker- Safe Havens.

2. What are the new privacy issues?

The high status of the confidentiality of personal biomedical information and the arguments for the non-use or non-disclosure of such information for secondary uses, in the absence of valid express consent, has been presented above. New information technologies and 'big-data' science raise new challenges. These include issues in relation to security and the risks of re-identification.

A second concern relates to the potential wider dissemination of data beyond health services and the medical research community. The potential uses of patient derived data for non-health purposes or for commercial purposes raises questions in relation to a patient's rights to control disclosures for such purposes.

3. What is the impact of developments in data science and information technology?

Public confidence in the security and in the boundaries around who should have access to such data and for what purpose will be a significant factor in realising the public benefits of future developments.

4. What are the opportunities for, and the impacts of, the use of linked biomedical data in research?

While it is for other experts to comment on the opportunities arising from such developments, PAC is aware of current and potential public health benefits from technologies such as pseudonymised data extraction, data mining and linkage.

Concerning pseudonymised data, public confidence in the security and in the risks of re-identification will be a significant factor in realising the public benefits of the use of linked biomedical data for research.

Where it is proposed to seek patient identifiable data for research uses, that patient's consent should normally be sought, unless there is a statutory basis justifying such uses, for example Section 251 of the NHS Act.

5. What are the opportunities for, and the impacts of, the use of linking biomedical data in medical practice?

While it is for other experts to comment on the opportunities arising from such developments PAC is aware of current and potential direct care benefits from the use of linking biomedical data in medical practice.

Direct care of that individual. Public trust in the security and confidentiality of any and all proposed developments is essential for success. Developments of this kind often create new risk scenarios requiring public protections beyond the original, usually implied consent, by which the information, typically for a patient's health record, was first obtained; for example linkages between primary care and hospital records. On the issue of suitable safeguards the Article 29 Data Protection Working Party[2] advises "the patient's self-determination concerning when and how his data are used should have a significant role as a major safeguard" (13/22). As a remedy the Working Party suggests "the possibility to express self-determination could – depending on the situation – also be offered in form of an opt-out/ a right to refuse" (14/22).

Research uses from information on episodes of treatment. See comments in response to question 4 above.

6. What are the opportunities for, and the impacts of using biomedical data outside biomedical research and health care?

It is for others to comment on the opportunities.

On the ethical implications see comments on questions 2 and 3 above.

7. What legal and governance mechanisms might support the ethical linking and use of biomedical data?

This is a key question in relation to the consultation.

Ethical principles. As stated at the outset of our response, patient confidentiality and informational privacy are pivotal considerations both in their own right and in seeking to realise the opportunities from the use of biomedical data for the public good. The nature of the obligation to protect confidentiality can be expressed in terms of three core principles[3]:

- Individuals have a fundamental right to the confidentiality and privacy of their health information;
- Individuals have a right to control access to and disclosure of their own health information by giving, withholding or withdrawing consent;
- For any proposed disclosure of health information have regard to its necessity, proportionality and any risks attached to it.

Information Governance. The use of anonymised and pseudonymised (de-identified) biomedical data provides significant opportunities for a range of secondary health and health services purposes including research. Effective, regulated processes for anonymisation and data extraction are required within primary care, hospital and approved safe havens. Regulated honest broker provision, typically from within safe havens, can further enhance the range of opportunities for secondary uses, including data linkage.

All of the forgoing processes require effective information governance. The recently issued Caldicott Review[4] greatly informs the requirements of information governance – "Dame Fiona's review has given us a tremendous opportunity to get information sharing right. At the same time, it is vital that we respect people's privacy and put them more in control of how their information is used. This is a fine balance, but an achievable one."[5]

Legislation. The duty of confidentiality is both ethical and legal, underpinned by the common law duty of confidentiality.

To enable essential secondary uses and disclosures of health care information, powers to exceptionally set aside the common law duty of confidentiality are currently provided within Section 251 of the NHS Act 2006 and more recently to the Information Centre in the Health and Social Care Act 2012. It should be noted that these provisions apply only in England and Wales. In Northern Ireland the Minister for Health has recently approved the development of relevant legislation. The need for additional regulations will need to be kept in view with respect to proposals emerging from the present consultation.

Additional Comments

1. It is important that the present consultation and any emerging recommendations are UK wide. This will more likely benefit all UK citizens, not only by their inclusion but in addressing a much larger population base sharing a common NHS. In addition there are frequent movements of citizens within and throughout the four countries of the UK.

2. We recommend that consideration is given to the inclusion of social and social care information within this consultation. In Northern Ireland there has been an integrated approach to health and social care for many years. This is the direction of travel for the rest of the UK.

The issues are in our experience very similar. Social and social care information is usually just as sensitive as health and medical information. The opportunities and potential benefits to be derived from secondary uses of such information are likely to be considerable. Issues being considered in this consultation ought, for the twenty-first century, to be addressed to bio-psycho-social and health data.

References

1. PAC was established in 2006 to advise Northern Ireland's Health and Social care Community on confidentiality issues**,** including new uses of personal information**.** Our comments have been informed by the Northern Ireland Code of Practice on Protecting the Confidentiality of Service User Information (Department of Health Social Services and Public Safety January 2012). This revised Code of Practice was developed by the Privacy Advisory Committee, following a comprehensive round of public consultation in 2011.

2. Article 29 Data Protection Working Party Working Document on the processing of personal data relating to health in electronic health records (EHR) (00323/07/EN WP 131). This Working Party was set up under Article 29 of Directive 95/46/EC.

3. Code of Practice on Protecting the Confidentiality of Service User Information (Department of Health Social Services and Public Safety - January 2012)
http://www.dhsspsni.gov.uk/confidentiality-code-of-practice0109.pdf

4. Information: To Share or not to Share. The Information Governance Review 2013

5. Jeremy Hunt MP (2013) Information: To Share or not to Share. Government Response to Caldicott Review. Department of Health