

Data Sharing Review

Richard Thomas and Dr Mark Walport

Consultation paper on the use and sharing of personal information in the public and private sector

Section 1: Background

Question 1. Please explain your interest in information sharing

Comments:

The NCRI Informatics Initiative aims to facilitate better access to the data generated in all areas of cancer research from genomics to clinical trials. To achieve this goal we aim to provide the cancer research community with an IT Infrastructure called the Informatics Platform.

The Informatics Platform will consist of an enabling infrastructure called the NCRI Oncology Information Exchange (ONIX). ONIX will connect data sources, services and tools forming an integrated research environment that will allow scientists to discover, share, analyse and re-use data.

A significant amount of data generated in cancer research includes personal information. This is usually generated in the clinical, bio-banking and epidemiology domains. ONIX endeavours to provide access to this information which will more than likely be anonymised to protect the identity of patients. ONIX will not store this data but simply acts as the software that will connect data housed in different locations and allow information to be shared between users that have appropriate access rights.

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2. What in your view are the key benefits of sharing personal information?

Comments:

The key benefits of sharing personal information collected in cancer research are it:

- Allows the linkage of information to different fields of research increasing our understanding of the factors that contribute to cancer development;
- Prevents duplication of research effort;
- Fosters collaboration and better working relationships between doctors, nurses, and researchers;
- Provides a rich source of data if information from different sources can be shared and combined;
- Enables patients/volunteers to make a significant contribution to medical research that

goes far beyond their original expectation;

- Increases the quality and methods of data collection so that data sets are full, easily interpretable and of a high standard; and
- Maximises the 'return' on data gathered

Question 3. What in your view are the key risks of sharing personal information?

Comments:

The potential risk of sharing personal information in cancer research is a patient's identity could be inadvertently disclosed either by a security breach or deductive disclosures. This could lead to the release of sensitive medical information that could cause distress or embarrassment.

Question 4. What scope and methods of personal information sharing, in your view, pose the greatest opportunities or risks?

Comments:

The methods that pose the greatest opportunities for the sharing of personal information include the development of IT systems that make the collation, discovery, sharing, transfer and access of information easier. For these systems to be truly effective security measures need to be in place to protect sensitive information and reduce the risk of security breaches.

In addition to IT systems, individual organisations need to develop clear policies, agreements and strategies for the sharing of personal information and they need to be monitored and adapted regularly to ensure that they continue to be relevant as situations and times change.

Training should be in place for all those who collect and use personal information so that they are fully aware of the implications of sharing personal information and what their responsibilities are. Training should be extensive enough to ensure that the relevant people are fully aware of the procedures associated with the sharing, handling and management of personal information to prevent security breaches.

Additionally, awareness/training campaigns should be implemented for patients/general public so that they have a better understanding of the information sharing process which would perhaps improve their attitude towards information sharing.

Section 3: The legal framework

Question 10. How valuable do you believe the second principle is?

Comments:

The second principle in the Data Protection Act is valuable in preventing the abuse of personal information and not allowing information to be used in a way that the individual would not agree to, but there needs to be some flexibility for medical research purposes to allow unforeseen credible areas to be explored as a follow-up to the initial specified purpose.

Section 4: Consent and transparency

Question 17. What if any barriers would a requirement for gaining consent create to the sharing of personal information?

Comments:

In the cancer research field it is standard practice to obtain consent to obtain, hold and use personal information and provided that there is proper planning so that consent is obtained early on there is usually no major problem. Patients are usually willing to share their personal information as long as it is anonymised and will be used for a good cause. The only barrier that could exist is if further consent is needed to explore areas that were not covered by the initial study. Having to obtain consent again would result in a time delay or a missed opportunity to explore further areas and incur additional labour cost/burden.

Question 18. Do you have any suggestions on how to make the sharing of information more transparent?

Comments:

In order to make the sharing of information more transparent organisations should publish statements that explain their policy on and strategy for information sharing. They should also describe the reasons behind their policies/strategies to illustrate to the public what the benefit to society is of allowing their data to be shared. In addition, they should actively publicise these statements and also develop concise, understandable publications about their information sharing process which they can distribute to the general public e.g.: brochures or frequently asked questions.

Prior to the collection of personal information, organisations should make certain that individuals understand who will have access to their information, what exactly they will have access to and what their information could be used for.

Question 19. How can we best ensure that information sharing policy is developed in a way that ensures proper transparency, scrutiny and accountability?

Comments:

During the development of the policy all those with an interest in information sharing should be consulted to ensure that they are able to make a contribution to the development of the policy. One method that could be used is the formation of Focus Groups to allow the opinions of a diverse range of people to be collected. This would guarantee that the views of the community are taken into account; it would allow in-depth discussion around particular sensitive issues and provide an opportunity to explain to the public the rationale behind the content of the policy.

Section 5: Technology

Question 20. What impact in your view have technological advances had on the sharing and

protection of personal information? Please provide examples?

Comments:

Technological advances have allowed for the development of secure databases to house large amounts of personal information and allow faster and easier transmission and analysis of information.

Unfortunately public sentiment to the fact that these technological advances mean that there could be a number of databases containing their personal information is not good; some feel that this is an invasion of privacy. Organisations therefore need to be more open about how long they store information for, what information they are storing and if they intend to share that information with another organisation. Increased transparency and greater public awareness efforts would alleviate some of the concerns that the public have about how much of their personal information is in circulation.

Question 21. Should the law mandate specific technical safeguards for protecting personal information

Comments:

The law should stipulate that sensitive information should be protected using the appropriate security measures whether it be password authentication, data encryption, firewalls etc. The law could also recommend regular security audits to ensure that systems and procedures are effective and remain relevant.

Question 22. How, in your view, could privacy enhancing techniques such as the anonymisation or pseudonymisation of personal information, help safeguard personal privacy, whilst facilitating activities such as performing medical research.

Comments:

Anonymisation and pseudonymisation is a technique used widely in cancer research and has proved a very effective way of protecting the identity of patients; encouraging patients to consent to the use of their personal information and allowing essential research that involves personal information to be conducted.

Section 6: International comparisons

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments:

Question 28.

Comments:
