ICR The Institute of Cancer Research

The use of patient data in research

Position Statement from
The Institute of Cancer Research, London

Summary

Access to patient data is vital for the research conducted at The Institute of Cancer Research (ICR). Patient data must be stored safely and securely to ensure patient confidentiality. But such safeguards to confidentiality must not come at the cost of efficient access to patient data for research use. We believe the regulatory system is too risk adverse in its requirements for explicit patient consent where research has been ethically approved. Research at the ICR has been delayed while waiting for approval to access patient data because of the complex regulation involved, particularly where initial consent was collected at the start of a long trial, and current norms on data use have developed since initial consent was collected. We are supportive of moves to clarify and streamline processes to access patient data for ethically approved clinical research.

July 2013

Patient data in research

Background information

The availability of large patient data collections is vital for research into cancer. The ICR's work includes epidemiological studies to identify causes of cancers, analyses of genetic information to identify potential drug targets and inform the management of patients, and clinical trials of potential new medicines and therapies. Cancer research has led the way in the application of genetics to disease risk and treatment, and this requires access to large sets of patient data including genetic information.

Public surveys show the vast majority of NHS patients would be willing for their data to be used for academic research purposes with appropriate safeguards on privacy. Patient data can include sensitive information such as health information, or personal information such as date of birth, NHS number or address. It is typically categorised as follows:

- **Identifiable** patient records include information allowing a patient to be identified. Access to identifiable patient data currently requires patient consent, except in exceptional circumstances, where approval is instead requested from the Secretary of State for Health.

- **Pseudonymised** or key-coded records have had all identifying data removed and can only be traced back to individuals using a 'key' which can be securely stored separately from the patient data.

- Patient data can be **anonymised** to remove any identifying information. As it cannot be linked back to an individual, accessing anonymised data for ethically approved projects does not currently require patient consent.

An Information Governance Review, carried out by an independent panel on behalf of the Secretary of State for Health, was published in April 2013. The review panel proposed a new framework to clarify how data should be shared and accessed for research:

- **Data for publication** must be anonymous/de-identified.

Patient data in research

- For **personal confidential data that is identifiable**, researchers must have consent to use the data and to share further. Data that will be linked with other data sets must be linked through an accredited safe haven.

- Pseudonymous data or anonymous data that can be easily re-identified has been reclassified as **de-identified data for limited disclosure or limited access**. Researchers using data must enter a contractual agreement between data controllers covering data flow, purposes of use, and safeguards. The data can be shared within an environment covered by a contractual agreement.

In the UK, the Data Protection Act, based upon the European Data Protection Directive, governs use of patient data in research. In 2012 the European Commission proposed to replace the directive with a Data Protection Regulation, which is currently in development.

Patient data in research

Key ICR positions on the use of patient data in research

- The ICR welcomes amendments to the NHS constitution in March 2013 including a default assumption that patient data collected by the NHS can be **anonymised** for use in ethically approved research, while allowing patients to opt out.

- The ICR believes individual patient consent should not be necessary to use **pseudonymised data** in ethically approved research.

  There is ambiguity over the regulation of pseudonymised data in proposed updates to the EU Data Protection Regulation, which could leave the regulation of pseudonymised data comparable to that of identifiable data. An enormous regulatory burden would be put on researchers to collect consent for every new use of pseudonymised patient data. This would delay use of large patient data sets such as the Clinical Practice Research Datalink (CPRD). It would also hinder large collaborative projects such as the Collaborative Oncological Gene-environment Study (COGS), involving more than 200,000 individuals, in which the ICR participates. We recommend this is addressed as the Regulation is revised.

  Currently, data access request forms are used to manage the sharing of pseudonymised data. The Information Governance Review introduced the idea of a legal contract to govern the sharing of pseudonymised data. We question whether this would improve existing practice and would like further details of how this would work in practice.

- **Identifiable** patient data must be stored safely and securely to ensure patient confidentiality and public trust in the use of personal data. We support the recommendation in The Information Governance Review that linked sets of personal confidential data should be stored in secure environments such as ‘safe havens’. We agree that contractual agreements between parties covering the use and storage of the data are

required when sharing identifiable patient data, to ensure that all parties store and use data safely, securely and appropriately.

- Regulations governing access to identifiable patient data can be overly burdensome and cause delays to research. Regulators should be less risk adverse around granting the use of patient data without explicit patient permission if the research has been ethically reviewed, and if appropriate safeguards for confidentiality are in place.

- There is concern that the proposed EU Data Protection Regulation could require further explicit consent for use of data collected many years ago, which would be time consuming, costly and prohibitive to our research. Article 83 of the Regulation, governing the processing of data for historical, statistical and scientific research purposes, changes the wording from 'consent' to 'specific, informed and explicit consent', apparently ruling out use of data in secondary research which has been ethically approved. Clinical trials for cancer treatments may take 10 or 20 years to complete and epidemiological studies longer. By the end of the trial the initial patient consent sometimes no longer covers current practices around data use. We recommend that this is recognised by ethical committees and that consent need not be sought retrospectively over the use of patient data in circumstances that were covered by the initial consent. Otherwise, it may be impossible to collect long-term outcome data or carry out long-term follow-ups, for patient benefit.

- We need to avoid the overly burdensome 'consent for consent' model for accessing identifiable patient data. Some researchers have had to ask consent from patients to view their records to select who to invite to take part in studies, and others have been prevented from contacting patients to ask for consent because contact details could only be released with the patient's consent. We are supportive of reforms to the NHS Constitution committing the NHS to inform patients of research studies for which they are eligible, with the assumption that patients are content to be approached.

- The Information Governance Review recommends following the Human Genetics Commission principle that 'private personal

genetic information should generally be treated as being of a confidential nature and should not be communicated to others without consent except for the weightiest of reasons'. We agree with this principle and recommend that all holders of genetic information treat personal genetic information as confidential information.