

Sharing patient data: exploring consensus on reasonable expectations

July 2017 - Seminar Report

Background

The National Data Guardian and her panel of advisors have been undertaking work to examine the circumstances under which health and care data may be legitimately shared, and the role that patients' reasonable expectations play in shaping these circumstances.

During this work, concerns have been raised that implied consent is being used as a justification for using and sharing information about patients for purposes which might not be regarded as direct care and where it may not be reasonable to expect that the patient understands how data about them is being used and shared.

To address some of these concerns, the National Data Guardian and Sheffield Solutions at The University of Sheffield agreed to host two seminars. The first of these was in Sheffield on 17 July 2017. It brought together an invited audience of clinicians, legal experts, ethicists, academics, and patient representatives to discuss the circumstances under which data may be legitimately shared, and the role that reasonable expectations play in shaping these circumstances.¹ The aim was to discover whether there is a consensus across these groups about a possible way forward.

This report presents the remarks made by speakers on the day and a flavour of the discussions exploring whether and to what extent there was consensus among attendees.

What is the problem?

It is a long-established principle of medicine that doctors must keep confidential the information provided by patients in their care. This principle is supported by law as well as professional regulation.² The common law duty of confidence entitles a patient who consults a doctor to have a reasonable expectation of privacy and this requires the doctor to maintain confidentiality, except in certain circumstances. A frequently used exception

¹ The event was organised in the wake of lively correspondence provoked by articles on the NDG's website by panel member Dr Alan Hassey, exposing a wide range of views about people's reasonable expectations:

<https://www.gov.uk/government/speeches/reasonable-expectations>

<https://www.gov.uk/government/speeches/exceeding-expectations>

² In April 2017 the General Medical Council published revised confidentiality guidance:

http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp

is when a GP refers a patient to a consultant and provides information about the patient that the consultant needs to know. The patient's consent for confidential information to be shared in this way does not have to be explicit. For legal purposes, implied consent may be sufficient.

The report of the Information Governance Review (IGR) that Dame Fiona conducted for the Department of Health in 2013 explained how healthcare professionals could share information about a patient on the basis of implied consent *“if it is reasonable to expect the patient understands how the information will be used.”*³

The IGR said:

“There are three tests for establishing the conditions under which consent can be implied, all of which must be met affirmatively:

- *Is the person sharing the information a registered and regulated professional or one of their direct care team?*
- *Is the activity a type of direct care within the scope specified by the professional's regulatory body?*
- *Does the professional have a legitimate relationship with the person or persons concerned?”*⁴

For many years the NHS has depended on implied consent to allow information about patients to flow among the teams of doctors, nurses, therapists and the ancillary staff working under their direction to provide individual care. This approach appears to have been accepted by patients and it has not been challenged in the courts. There is no desire to remove this underpinning of the arrangements for managing the confidentiality of the hundreds of thousands of patients who use NHS services every day, doing so in a way that permits relevant information to be available to the teams providing care.

However, the National Data Guardian has become aware that the boundaries of implied consent described in the IGR are coming under strain. In some cases implied consent is being used as a justification for using and sharing information about patients for purposes that cannot be regarded as direct care. Even when information is used and shared for direct care purposes it may not always be reasonable to expect that the patient understands how data about them is being used and shared as advances in medical practice and technology lead to new ways of delivering care. Many of these activities have laudable aims. They may lead to medical breakthroughs or improvements in the way services are delivered. Are these benefits to be lost because these activities do not satisfy the conditions for reliance on implied consent? Or is there a more helpful approach that allows progress to be made while maintaining patients' confidentiality and trust?

Examples of new ways of working where the existing model of implied consent is coming under strain include:

³ Information Governance Review, Executive Summary, page 12

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

⁴ Information Governance Review, Chapter 5, page 56

- The need for information about patients to flow more freely across organisational boundaries in order to provide patients with integrated care tailored to meet their individual needs;
- Developments in genetic and genomic medicine that blur the boundary between direct care and other purposes;
- Increasing reliance upon multi-disciplinary teams with specialists geographically distant from individual patients.

Questions that baffle GPs

The seminar heard from **Dr Arjun Dhillon**, a practising GP and Deputy Caldicott Guardian at NHS Digital. He said clinicians remain firmly committed to maintaining their patients' confidentiality. They believe in it and their professional good standing depends on it. However, developments in technology, legislation, clinical practice and healthcare redesign have left many frontline clinicians uncertain how to deal with issues that frequently confront them.

Examples of questions that GPs frequently ask themselves include:

- Should I share the patient's whole care record with other NHS professionals?
- Should I share large extracts with public health-commissioned services such as diabetic retinopathy screening?
- Can I send referrals to a private company providing referral facilitation service? Is this direct care?
- Should I share an extract of all my records with the local care record service for direct care under implied consent?
- Is it right that the local care record service can then anonymise that data and use it for secondary uses without explicit patient consent?

The problem is not that GPs do not trouble to find out what to do. The answers to these questions are not clear to everyone. Nor is it apparent who is taking responsibility for answering them, or how this work will be funded.

Issues that concern clinical genetics professionals

In her annual report published in July 2017⁵, Dame Sally Davies, the Chief Medical Officer, called for DNA testing of cancer patients and people with rare diseases to identify specific disease-causing genetic variations. This would allow for quicker and more accurate diagnosis and for treatment to be tailored more specifically to their individual needs. Dame Sally said that within three to five years centralised laboratories should be established to handle widespread DNA testing, and genetic testing, and where applicable, screening should be integrated into standard treatment. In a paper published in August this year, the NDG explored how a consensus might be progressed on data sharing to support NHS clinical genetics and genomics services⁶.

⁵ <https://www.gov.uk/government/publications/chief-medical-officer-annual-report-2016-generation-genome>

⁶ <https://www.gov.uk/government/publications/developing-a-consensus-on-data-sharing-to-support-nhs-clinical-genetics-and-genomics-services>

Alison Hall, Head of Humanities at the PHG Foundation, explained that there is lack of agreement concerning what geneticists can and cannot do within the law to share genomic information that may identify an individual. Surveys of NHS genetics services in 2015 and 2016 showed this uncertainty was impeding data sharing that would be beneficial to patients for their safe and effective care. It is through the sharing of such information, potentially across a wide geography, that iterative interpretation of the significance of specific gene variants becomes possible. The sharing of genetic information about one patient may well help to improve diagnosis and care for other patients and usually the increased knowledge that such sharing brings will be of patient benefit. But can the consent of the individual whose information is being shared be implied if there are instances when sharing may not benefit the direct care of that individual?

Hall explained the difficulties in the field of genetic medicine to distinguish between sharing patients' data solely for those patients' own direct care, sharing data for others' direct care and sharing data for research. In view of this, a key challenge is to secure public trust and confidence.

A possible solution

The central proposition examined was that there is a need for close consideration of the role played by "reasonable expectations" in the legal tests for lawful use. This might help to establish more clearly a suitable legal justification for information sharing to support worthwhile initiatives to integrate patient care or develop new health technologies.

Dr Mark Taylor, Senior Lecturer in Law at The University of Sheffield and a member of the National Data Guardian's Panel of advisers posed a key question at the start of the day: would it be useful to re-examine the reasonable expectations of patients to find out whether they expect information about them to be shared in certain circumstances, as well as expecting that information to remain confidential in other circumstances? If the answers to these questions is yes, then work can start on discovering what are patients' reasonable expectations for data sharing currently - and what they might become if professionals and organisations do more to explain how health and care practices are developing. The 'reasonable expectations' that emerged from such work could, through professional guidance, be related to existing legal concepts controlling use of confidential patient information.

Dr Taylor reviewed recent precedents showing how the courts have dealt with cases involving the Common Law Duty of Confidence. They show that the question of a reasonable expectation of privacy has come to the fore in recent years. In assessing whether an individual has a reasonable expectation of privacy the courts will consider whether the information is protected by Article 8 of the European Convention of Human Rights, which recognises an individual's right to respect for private and family life. If it is established that an individual does have a right to privacy, the courts will then take a view on whether an individual's rights have been breached. Dr Taylor suggested that the recent case of *R (on the application of W,X,Y, and Z) v Secretary of State for Health [2015] EWCA Civ 1034*⁷ raises the possibility that the common law duty may be abated

⁷ <https://www.judiciary.gov.uk/wp-content/uploads/2015/10/w-x-y-z.pdf>

when there is no (longer any) reasonable expectation of privacy in the circumstances. The effect would be to permit disclosure of information in circumstances that would otherwise be a breach of confidentiality. This potentially extends the circumstances under which disclosure is lawful beyond the possibilities of 'consent', statutory authority, or overriding public interest. The 'reasonable expectation of privacy' creates a duty of confidence, but is it correct to consider that a reasonable expectation that data would be shared may also be grounds for lawful disclosure?

Alternative viewpoints

Aspects of Dr Taylor's thesis were challenged by other speakers. **Ruth Boardman**, co-head of international data protection practice at solicitors Bird & Bird LLP, was cautious about his interpretation of recent judgements. She said there was potential for "reasonable expectations" to develop to fulfil the role that Dr Taylor described. "But given the cases we have had to date, I don't think we are there yet. If you decide that is the direction of travel, how do you generate enough certainty to allow people to share data relying on a reasonable expectations approach?"

Baroness O'Neill, Professor Emeritus at University of Cambridge, was unable to attend in person, but an address that she had prepared for the seminar titled "Is Data Protection Obsolescent?" was read out to participants.

Her remarks highlighted challenges around a data protection approach to safeguarding privacy: "For over 30 years privacy protection has been addressed in the EU and elsewhere by legislating for data protection. The approach has never been easy, in part because the right to privacy (like most human rights standards) is a *qualified right*, but also (and increasingly) because of technological and other changes, particularly in data systems and management, which are placing increasing strain on data protection approaches to privacy."

Baroness O'Neill indicated that she was inclined to think that reducing reliance on data protection may be the best way forward and that other approaches are imaginable, for example placing more emphasis on confidentiality.

Baroness O'Neill also emphasised that if one is to use the phrase 'reasonable expectation', then one should be explicit about what may constitute robust and reliable evidence to support the claim. Her address noted that "...Expectations are formed relative to some evidence base. Reasonable expectations may reflect an accurate understanding of a reliable evidence base, or a poor understanding of that evidence base; an accurate understanding of an unreliable evidence base, or a poor understanding of an unreliable evidence base."

Her address closed by reminding seminar attendees that "Trust is only worth having if it is placed in matters in which others are trustworthy; equally mistrust is worth having when it is directed at matters in which others are indeed untrustworthy." She emphasised that what matters is not persuading people to trust but establishing clear standards against which evidentially robust evidence may be offered - those who care about privacy or other

qualified rights must first think about ways to secure trustworthy management and use of data and not seek simply to support public confidence by persuasion.

In a wide ranging address **Jonathan Montgomery**, Professor of Health Care Law at University College London and Chair of the Health Research Authority, looked at privacy rights under Article 8 of the European Convention on Human Rights.

He said they were not dependent either on the nature of the information about the patient, nor on the relationship between the patient and the professional. What mattered was the impact on the patient's private and family life. The impact would be objectively assessed by the court in relation to whether a reasonable person would feel justifiably aggrieved.

The questions at stake were these:

1. Are rights engaged?
2. Are they infringed?
3. If so, is there a 'legitimate purpose'?
4. If so, is the infringement 'proportionate'? (Reasonable expectations relevant here?)
5. If so, is it 'in accordance with the law'?

The method for the public engagement element of this work was explained by **Dr Malcolm Oswald**, Director of Citizens Juries Community Interest Company (CIC). This company has been commissioned by the NDG and Connected Health Cities to run a citizens jury to explore the subject of reasonable expectations. This will involve 18 members of the public, drawn from a range of backgrounds, spending three days considering what uses of health and care data they would expect and accept. The jury will be assisted in its deliberations by expert witnesses and a steering group will be charged with minimising any bias in the materials and information given to the jury. The aim will be to understand both what data uses the participants will support and why. This piece of deliberative engagement will be supplemented by a larger scale opinion survey.

Conclusions

Within the time available, attendees at the seminar reached a tentative consensus that the concept of 'reasonable expectations' merits further exploration from a legal, clinical and patient perspective to assess its potential.

Participants were struck by a mismatch between what clinicians regard as necessary and routine and what patients say they expect. Patients want the services caring for them to share information effectively and are surprised when they do not. Yet the seminar heard that patients may be surprised to hear about activities that clinicians regard as standard practice, such as dictating letters about patients for typing up by clerical staff overseas. Further work with clinicians and other health and care professionals may help to establish what information sharing they think they need to deliver better care. Further work with patients might then establish whether they understand and accept those requirements. Some participants believed that some particular clinical demands for information sharing should be non-negotiable and patients should be asked accept them as part of a 'social contract'. However, there was not time to explore this approach in detail.

It should be acknowledged that Dr Dhillon did not get answers to the questions about information sharing that are perplexing his GP colleagues, nor was a clear conclusion reached about how the challenges posed by Alison Hall might be resolved. This points to the need for further work in this area to explore whether the legal approaches and principles supported on the day might help to meet the clinical challenges and uncertainties.

On the legal side, the seminar ended with agreement among participants on the day that Dr Taylor's interpretation of the law of reasonable expectations deserved further exploration. If his interpretation gains traction, it would not be necessary to wait for the courts to decide cases to create common law precedent. Participants noted that it would be possible for the Department of Health, NHS England or professional bodies to develop new institutional norms by updating policy and revising professional guidance.

Next steps

A second seminar exploring how health and care professionals may share personal data in line with patients' reasonable expectations was held in October 2017 and a separate report of this event will be published. The NDG is also planning further events to engage with clinicians and members of the public. The aim will be to determine the content of "reasonable expectations" from their respective perspectives. These events will provide opportunities to test the effectiveness and utility of the different legal approaches described above and explore whether it is possible to build a reliable evidence base to underpin referral to reasonable expectations with a trustworthy data management approach. How well do they protect the expectations that are recognised as reasonable in fact by health and care professionals, patients, and members of the public?

About the organisations

The National Data Guardian

The National Data Guardian (NDG) advises and challenges the health and care system to help ensure that citizens' confidential information is safeguarded securely and used properly. Dame Fiona Caldicott was appointed as the first National Data Guardian for health and care by the Secretary of State for Health, Jeremy Hunt, in November 2014. The NDG's role is to help make sure the public can trust their confidential information is securely safeguarded and make sure that it is used to support citizens' care and to achieve better outcomes from health and care services.

Sheffield Solutions

Sheffield Solutions is an initiative of the Faculty of Social Sciences at The University of Sheffield. It supports events, activities and outputs that connect social science perspectives to policy makers, practitioners and other external audiences in order to tackle pressing global issues. For further information, contact sheffieldsolutions@sheffield.ac.uk

Sheffield Solutions is in part supported by The University of Sheffield's ESRC Impact Accelerator Account.

Summary of terms

The terms and definitions used in this paper are based on those used in the Information Governance Review 2013⁸ and National Data Guardian Review of Data Security, Consent and Opt-Outs 2016⁹.

Anonymise: To rendering data into a form which does not identify individuals, or which makes the risk of re-identification sufficiently low in a particular context that it does not constitute personal data.

Consent: The informed agreement for something to happen after consideration by the individual. For consent to be legally valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily. In the context of consent to share confidential information, this means individuals should be aware and understand how their information is to be used and shared (there should be ‘no surprises’), and they should understand the implications of their decision, particularly where their refusal to allow information to be shared is likely to affect the care they receive. This applies to both explicit and implied consent. See the Information Governance Review for definitions of explicit and implied consent.

Data Protection Act 1998 (DPA): The Act of Parliament which regulates the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information.

Data sharing: The disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. This can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose or for exceptional, one-off decisions to share data for any of a range of purposes.

Direct care: Defined in the Information Governance Review as a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals’ ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, and person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team, with whom the individual has a legitimate relationship for their care.

General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) is the new EU Regulation 2016/679 adopted by the European Parliament and

⁸ <https://www.gov.uk/government/publications/the-information-governance-review>

⁹ <https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs>

Council, which is intended to strengthen and unify data protection for individuals within the European Union.

Indirect care or secondary uses: Activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine, and medical research. Examples of activities are risk prediction and stratification, service evaluation, needs assessment, and financial audit.

Information Governance Review: Following a request from the Secretary of State for Health, Dame Fiona Caldicott carried out this independent review of information sharing to ensure that there is an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care. It is available here: <https://www.gov.uk/government/publications/the-information-governance-review>. The Government's response, which was published in July 2017, is available here: <https://www.gov.uk/government/news/government-responds-on-cyber-security-and-data>.

Secondary uses: See 'indirect care'