Department of Health

National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs

Public Consultation

July 2016

Title: National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs Consultation Document
Author: Data and Cyber Security Policy / Digital and Data / Innovation, Growth and Technology / 13630
Document Purpose: Consultation
Publication date: July 2016
Target audience: Public, professionals and health and care organisations
Contact details: NDGReviewConsultation@dh.gsi.gov.uk

Published to gov.uk, in PDF format only.

www.gov.uk/dh

July 2016

Foreword

Sharing the right information with the right people at the right time is essential to the delivery of high quality healthcare, whether in making an accurate diagnosis or in ensuring that test results are communicated and acted upon swiftly, or in making sure that the right social care package is in place to support someone to stay in their own home for longer. As all healthcare systems go digital, it is vital for:

a) individual diagnosis and treatment

b) system safety and performance, and

c) in research, to improve treatment and care for patients.

Whilst there is a big difference between a patients individual personal medical record and anonymous large-scale historic data sets (e.g. what % of the patients on a particular drug developed side effects over the last 10yrs), which patients understand, patients will rightly want to know that we are putting in place appropriate systems and safeguards to regulate different levels of consent, prevent inappropriate access to or use of information.

As health and social care organisations become increasingly paperless and digital, the opportunities to use data for the benefit of patients and the wider public increase significantly. It is also the case that a greater reliance on digital technology means that more robust data protection is needed to ensure patient trust and confidence and that these responsibilities must be taken seriously by the system and its staff. This is why, last September, we asked both the Care Quality Commission and Dame Fiona Caldicott, the National Data Guardian for Health and Care, to review data security across health and care. We also asked Dame Fiona to propose a number of new data security standards to be applied in all NHS and social care organisations, and to set out options for a new consent/opt-out model for data sharing, so that people clearly understand the choices available to them about how their personal confidential information will be used.

We warmly welcome the recommendations made in both the CQC and National Data Guardian's reports and are grateful for the input that many interested professional bodies, health and care organisations, stakeholders and members of the public have given.

In her report, Dame Fiona strongly recommends that the Government should consult the public on both the data security standards, and her proposals for a new consent/opt-out model, and we are pleased to take forward that recommendation in this document. We look forward to hearing your views about how we can build a more trusted and secure approach to the way in which health and care data is used, shared and protected.

Rt. Hon Jeremy Hunt MP
Secretary of State for Health

George Freeman MP
Minster for Life Sciences

July 2016

Contents

1. Introduction

1.1. The delivery of high quality health and care services has always depended on trust between patients and service users, and those who are providing their care. To a very significant extent, service delivery also relies on the flow of patient data between those with a legitimate interest in holding and using it. As health and social care services become more integrated, as more personal confidential data is held, and given the particular sensitivity of health and care data, it is more important than ever that people have a clear understanding about how and when information about them will be shared, how privacy is protected, and how the proper use of information will benefit them and others.

1.2. The report prepared by the National Data Guardian for Health and Care (NDG) considers two aspects of people's trust - whether data security is strong enough, and the basis upon which information is shared, and, particularly, whether people understand when they can consent or opt-out of their personal confidential information being used. In his speech to the NHS Innovation Expo on 2 September 2015, the Secretary of State talked about how NHS and social care organisations need to make better use of technology to empower patients to take a more active role in their own care. He went on to say that improved opportunities in digital technology and data use must be supported by improved data security. Only when we have the balance right between these two elements, will public trust in this vital area increase.

1.3. In this context, the Secretary of State commissioned a Review of data security and consent, asking the Care Quality Commission (CQC) to review current approaches to data security across the NHS, and Dame Fiona Caldicott, the NDG, to develop data security standards that can be applied to the whole health and social care system. Finally, he asked Dame Fiona to propose a new consent/opt-out model for data sharing to enable people to make an informed decision about how their personal confidential data will be used.

1.4. The Review recommended that the Department of Health should conduct a public consultation on the proposed security standards and consent/opt-out model. The Department also intends to bring forward Regulations later in 2016 which will allow the Health &Social Care Information Centre to improve the way information can be shared in specified circumstances. These Regulations will be the subject of a separate consultation later in the year.

1.5. This consultation is the beginning of a process to seek as wide a range of views as possible on each area of the NDG's Review. There will be a longer period of engagement with the public and professionals to complement this consultation.

1.6. Like the Review itself, this consultation covers both the proposed data security standards and the new consent/opt-out model, with questions relating to each area. You are invited to respond to both sections, or to whichever section or questions you have a particular interest in. You should not feel obliged to answer all the questions. Details of how you can respond to this consultation document can be found in section 6.

Introduction

Question 1: Please tell us which group you belong to

Question 2: If you are a member of an organisation or profession, please tell us if you are responding in a personal or private capacity

Question 3: If the Department of Health or other organisations were to create further opportunities to engage on data security and the consent/opt-out model, would you be interested in attending? If so where would you find it helpful an event to be held?

2. Data Security

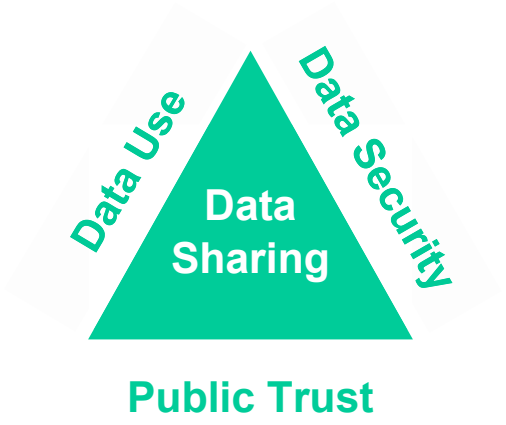
2.1. The NDG's Review showed that people generally trust the NHS to protect information. However there have been cases where that trust has been eroded by data breaches, where sensitive information has been shared inappropriately or without consent, or by people's individual experiences of misplaced or lost records.

2.2. As the health and social care system becomes increasingly paperless and digital it becomes ever more important that there are adequate and robust protections in place to protect the data and information held within it. Personal confidential data is valuable to those with malicious intent, and health and social care systems will continue to be at risk of external threats and potential breaches. There is widespread appreciation of the need for digital systems and a paper free NHS, but there are concerns that the move to digital systems increases the potential impact on organisations and individuals of any breaches.

2.3. Whilst there are examples of good practice and most organisations are concerned about data security, the Review heard of problems involving people, processes and technology. It found that data is not always adequately protected and individuals and organisations were not consistently held to account when breaches occurred.

2.4. The NDG's new model for cyber security is built upon the three pillars of people, processes and technology. Data breaches are often caused by people who are finding workarounds to burdensome processes and outdated technology, and may have a lack of awareness of their responsibilities. A strong Senior Information Risk Owner (SIRO) and an engaged board can make a significant difference, and where properly supported, the appointment of Caldicott Guardians has had a positive impact on staff being equipped to handle information respectfully and safely. With the right processes in place staff should be able to proactively prevent data security breaches and respond appropriately if there are incidents or near misses. Better technology which is secure and up to date, including the move to a paper-free NHS, is important in helping people to do the right thing.

2.5. Information sharing and technology have huge potential to improve the health and care system, but these opportunities will not be realised unless patients can trust the system to look after their information securely. The appropriate use of data must be complemented by strong data security. There is essentially a strong relationship between Data Use, Data Security, and Public Trust.



2.6. On the basis that data breaches are caused by people, processes and technology, the review recommends ten new data security standards:

Proposed Data Security Standards

1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.
2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.
4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
8. No unsupported operating systems, software or internet browsers are used within the IT estate.
9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
10. Suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standard.

Question 4: The Review proposes ten data security standards relating to Leadership, People, Processes and Technology. Please provide your views about these standards.

Question 5: If applicable, how far does your organisation already meet the requirements of the ten standards?

Please provide examples which might be shared as best practice

Question 6: By reference to each of the proposed standards, please can you identify any specific or general barriers to implementation of the proposed standards?

2.7. The NDG's Review recommends the introduction of ten data security standards for every organisation handling health and social care information, applying across the entire health and social care system, supporting rather than inhibiting data sharing. The standards are designed to address the principal root cause of existing breaches to paper-based and digital data, and to protect systems against potential future breaches to digital data.

Question 7: Please describe any particular challenges that organisations which provide social care or other services might face in implementing the ten standards

Question 8: Is there an appropriate focus on data security, including at senior levels, within your organisation? Please provide comments to support your answer and/or suggest areas for improvement

Question 9: What support from the Department of Health, the Health & Social Care Information Centre, or NHS England would you find helpful in implementing the ten standards?

2.8. The Review recommends that CQC should amend its inspection framework and inspection approach to include assurance that appropriate internal and external validation against the new data security standards have been carried out and make sure that inspectors are appropriately trained. HSCIC should use the redesigned "IG toolkit" to inform CQC of 'at risk' organisations, and CQC should use the information to prioritise action.

2.9. The review also heard from the primary care community in particular that they would value support to meet the standards provided by a refreshed IG toolkit and HSCIC. HSCIC could, for example, use the new toolkit to identify organisations that would benefit from additional support, and also to put organisations in touch with each other for peer support. HSCIC should work with other regulators to ensure that there is coherent oversight of data security across the health and social care system.

Question 10: Do you agree with the approaches to objective assurance that we have outlined in paragraphs 2.8 and 2.9 of this document?

3. The importance of data sharing

3.1. The health and care data collected by the NHS and the wider care system is a rich resource, with enormous potential to be used to drive improvements in health and care. However the benefits that can be derived from data sharing must be balanced against the need to keep data confidential. There is a clear tension between the principles of transparency and the desirability of sharing data on the one hand, and public concern about privacy and the potential for misuse of data on the other – especially in relation to the use of their personal confidential health data. Urgent work is needed to rebuild the public's trust in the health and care system's ability to manage their personal confidential data safely and securely.

3.2. The NDG's Review highlighted that the public are not fully informed or engaged in the issues around data sharing, and do not fully understand what options they have in relation to the use of their information. Likewise the Review pointed out how many health and social care professionals lack confidence in what they are allowed to do with personal confidential data and what can be shared with whom. These fundamental barriers must be addressed so that people can make informed decisions regarding their data, and professionals are able to use and share data in ways that benefit all.

3.3. The NDG proposes a new model which will enable people to opt-out from their personal confidential data being used for purposes beyond their direct care. These purposes may include the use of personal confidential data to provide local services and check the quality of care, and support for research to improve treatment and care. Under this model, people will still be able to give their explicit consent for specific research projects, as they do now, and ask that their health care professional does not share a particular piece of information with others involved in providing their care, as they do now. Once a preference is expressed it will, in time, be shared with all health and care organisations.

4. Proposed Consent/Opt-out Model

4.1. The Review summarised the recommendations for the new consent/opt-out model into the following eight statements.

1. You are protected by the law.

Your personal confidential information will only ever be used where allowed by law. It will never be used for marketing or insurance purposes, without your consent.

2. Information is essential for high quality care.

Doctors, nurses and others providing your care need to have some information about you to ensure that your care is safe and effective.

However, you can ask your health care professional not to pass on particular information to others involved in providing your care.

3. Information is essential for other beneficial purposes.

Information about you is needed to maintain and improve the quality of care for you and for the whole community. It helps the NHS and social care organisations to provide the right care in the right places and it enables research to develop better care and treatment.

4. You have the right to opt-out.

You have the right to opt-out of your personal confidential information being used for these other purposes beyond your direct care.

This opt-out covers:

d) Personal confidential information being used to provide local services and run the NHS and social care system.

For example:

- NHS England surveys, for example to find out patients' experiences of care and treatment for cancer
- regulators and those providing care checking its quality
- NHS Improvement auditing the quality of hospital data.

e) Personal confidential information being used to support research and improve treatment and care.

For example:

- a university researching the effectiveness of the NHS Bowel Cancer Screening Programme
- a researcher writing to an individual to invite them to participate in a specific approved research project

This choice could be presented as two separate opt-outs. Or there could be a single opt-out covering personal confidential information being used both in running the health and social care system and to support research and improve treatment and care.

5. This opt-out will be respected by all organisations that use health and social care information.

You only have to state your preference once, and it will be applied across the health and social care system. You can change your mind, and this new preference will be honoured.

6. Explicit consent will continue to be possible.

Even if you opt-out, you can continue to give your explicit consent to share your personal confidential information if you wish, for example for a specific research study.

7. The opt-out will not apply to anonymised information.

The Information Commissioner's Office has a Code of Practice that establishes how data may be sufficiently anonymised that it may be used in controlled circumstances without breaching anyone's privacy. The ICO independently monitors the Code.

The Health and Social Care Information Centre, as the statutory safe haven for the health and social care system, will anonymise personal confidential information it holds and share it with those that are authorised to use it.

By using anonymised data, NHS managers and researchers will have less need to use people's personal confidential information and less justification for doing so.

8. The opt-out will not apply in certain exceptional circumstances.

The opt-out will not apply where there is an overriding public interest, such as preventing and responding to natural disaster; monitoring and control of important diseases in humans such as TB and diseases of epidemic potential such as Ebola; infections that pass between animals and humans such as the zika virus; and for chemical, biological, radiological and nuclear events. It would also include personal confidential data for monitoring and control of communicable diseases and other risks to public health.

The opt-out will not apply where there is a mandatory legal requirement. This includes:

- the Care Quality Commission, which has powers of inspection and entry to require documents, information and records;
- the HSCIC, the statutory safe haven, which has powers to collect information when directed by the Secretary of State or NHS England;
- the NHS Counter Fraud Service, which has powers to prevent, detect and prosecute fraud in the NHS;
- investigations by regulators of professionals;
- coroners' investigations into the circumstances of a death, i.e. if the death occurred in a violent manner or in custody;
- health professionals must report notifiable diseases, including food poisoning;
- the Chief Medical Officer must be notified of termination of pregnancy;
- employers must report deaths, major injuries and accidents to the Health and Safety Executive;
- information must be provided to the police when requested to help identify a driver alleged to have committed a traffic offence; or to help prevent an act of terrorism or prosecuting a terrorist;
- information must be shared for child or vulnerable adult safeguarding purposes; and
- health professionals must report known cases of female genital mutilation to police.

In addition the Review also sets out that the following should not be part of the opt-out:

- some forms of invoice validation where there is no alternative solution, such as the use of anonymised data;
- demographic information flows (e.g. NHS number, address) into the Office of National Statistics (ONS) for the production of official statistics e.g. to look at internal migration;
- national registers of disease including cancer where there will be a new approach to informing patients about registration.

Question 11: Do you have any comments or points of clarification about any of the eight elements of the model described above? If so please provide details in the space below, making it clear which of the elements you are referring to.

4.2. The Review has recommended that the Government should consider introducing stronger sanctions to protect anonymised data. These will include introducing criminal penalties for the deliberate or negligent re-identification of individuals. This is intended to give the public greater confidence that firm action will be taken as necessary to protect their personal confidential data.

Question 12: Do you support the recommendation that the Government should introduce stronger sanctions, including criminal penalties in the case of deliberate or negligent re-identification, to protect an individual's anonymised data?

Question 13: If you are working within health or social care, what support might you or your organisation require to implement this model, if applicable?

Question 14: If you are a patient or service user, where would you look for advice before making a choice?

4.3. The Review heard that people find the current options on consent difficult and confusing. They are looking for a clearer choice that is easier to understand. The new consent/opt-out model proposed by the Review will provide people with this less complex choice. HSCIC, soon to be renamed NHS Digital to reflect the vital role the organisation plays in delivering essential technology and information to improve health and care, will continue to be the statutory safe haven for the secure sharing of data, and the public can take confidence that their opt-out choices will be properly reflected by HSCIC as they make them.

4.4. At the moment, there are a number of different opt-outs, including Type 1 and Type 2 opt-outs and other objections and opt-outs housed in national and local computer systems. The Review is not recommending any changes to the existing arrangements until there has been a full consultation on the proposed new consent/opt-out model. However, once this consultation is complete, and the new model is in place, the Review recommends that existing arrangements should be replaced.

4.5. Some patients will have already made choices about the sharing of their information under the existing opt-out framework, and it will need to be decided how these opt-outs will be treated under any new consent/opt-out model.

Question 15: What are your views about what needs to be done to move from the current opt-out system to a new consent/opt-out model?

5. Equality Issues

5.1. Section 149 of the Equality Act 2010 establishes the Public Sector Equality Duty (PSED), requiring public authorities to have due regard to the need to:

- eliminate discrimination, harassment, victimisation and any other conduct prohibited in the 2010 Act;
- advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it; and
- foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

5.2. Section 149(7) of the 2010 Act describes relevant protected characteristics for the purpose of the PSED as: age; disability; gender reassignment; pregnancy and maternity; race; religion or belief; sex; and, sexual orientation. It also specifies that Ministers of the Crown and government departments are public authorities for the purpose of the PSED.

5.3. The Secretary of State for Health has a further duty: he must have regard to the need to reduce inequalities between the people of England with respect to the benefits that may be obtained by them from the health service.

5.4. In the development of the new policies proposed in this consultation, we must ensure that we have due regard to the three aims of the PSED and the Secretary of State for Health's duty to have regard to the need to reduce health inequalities. We hope to use this consultation exercise to obtain the views of stakeholders on possible impacts to inform the Department's work to meet its statutory equality duties.

Question 16: Do you think any of the proposals set out in this consultation document could have equality impacts for affected persons who share a protected characteristic, as described above?

Question 17: Do you have any views on the proposals in relation to the Secretary of State for Health's duty in relation to reducing health inequalities? If so, please tell us about them.

6. How to Respond

6.1. This section outlines the ways in which you can respond to this consultation.

6.2. This consultation is part of a wider programme of engagement and further opportunities will be made available throughout the consultation period.

6.3. It is therefore our intention to consult on the NDG's Review for a period of nine weeks, closing on 7 September 2016.

6.4. In response to this consultation, you can:

- Answer the questions online, National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs (http://consultations.dh.gov.uk/information/ndg-review-of-data-security-consent-and-opt-outs)
- Email your response to: NDGReviewConsultation@dh.gsi.gov.uk
- Post your responses to:
  NDG's Review of Data Security, Consent and Opt-Outs
  Room 2N12
  Quarry House
  Quarry Hill
  Leeds
  West Yorkshire
  LS2 7UE