Department of Health

Your Data:

Better Security, Better Choice, Better Care

Government response to the National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs and the Care Quality Commission's Review 'Safe Data, Safe Care'

July 2017

Title:

Your Data: Better Security, Better Choice, Better Care.
Government response to the National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs and Care Quality Commission's Review 'Safe Data, Safe Care'

Author:

Department of Health, Data Sharing and Cyber Security Team

Document Purpose:

To set out the Government's Response to the National Data Guardian's Review on Data Security, Consent and Opt-Outs, and the Care Quality Commission's Review 'Safe Data, Safe Care'. To provide a summary of consultation responses and set out the Government's proposed approach, moving forwards.

Publication date:

12 July 2017

Target audience:

Patients and members of the public
Health and care professionals
Providers and commissioners of health and care services
Medical research charities and other research organisations

Contact details:

Data Sharing and Cyber Security Team
Room 2N12
Quarry House
Quarry Hill
Leeds LS2 7UE

Email: I&Tbriefinghub@dh.gsi.gov.uk

Published to gov.uk, in PDF format only: www.gov.uk/dh

Contents

Foreword 2

Executive Summary 4

1. About the Consultation 9

2. Data Security Standards 10

3. Data Sharing and Opt-Outs 23

4. Equality Issues 38

5. Patient Empowerment 41

Annex A: Response to the National Data Guardian's Recommendations 43

Annex B: Response to the Care Quality Commission's Recommendations 49

Annex C: Consultation questions 51

Annex D: The National Data Guardian's 10 Data Security Standards 53

Annex E: The National Data Guardian's 8 Point Model 55

Annex F: Consultation Analysis and Summary of Responses 57

Annex G: Implementation Plan 65

Annex H: Glossary 75

Acknowledgments 79

Foreword

Making greater use of information and data enables health and care professionals to provide quality and safe care that improves our lives. It helps researchers unlock new treatments and make medical breakthroughs, and, it means our health and social care system runs effectively and efficiently. We all can understand, see and experience these benefits for ourselves, our families and friends.

We are rightly proud of our existing world-class science base which has helped to improve diagnosis and unlock new treatments, so that more people now survive the devastating effects of life-threatening and debilitating illnesses. However, we can, and must, do more to ensure that organisations are equipped for the twenty-first century. This means being resilient to data and cyber threats, and using patient information safely and securely. Getting this right underpins our ambition of having a world class health and social care system in the digital age.

The global WannaCry cyber attack in May 2017 has reaffirmed the potential for cyber incidents to impact directly on patient care and the need for our health and care system to act decisively to minimise the impact on essential front-line services.

Using data and sharing information are vital for important purposes such as safeguarding vulnerable people and we must strive to ensure that this is done securely and effectively by health and care organisations. We have heard that people support and can see the potential benefits of doing this.

With this in mind Dame Fiona Caldicott, the National Data Guardian for Health and Care, was asked to undertake a review of data security and data sharing in the health and social care system. Her report, *Review of Data Security, Consent and Opt-Outs* was published in July 2016 and we are delighted to respond to it.

We warmly welcome and support Dame Fiona's recommendations for new national data security standards, which underpin the resilience of the health and social care system to data and cyber risks; and, for giving people choice to opt out, if they wish, of their information being used for purposes beyond their direct care.

We also welcome and support the recommendations made by the Care Quality Commission's review *Safe Data, Safe Care.*

The Government's high-level implementation plan is already being taken forward by the Department of Health, working together with NHS Digital, NHS England, the Care Quality Commission, NHS Improvement and other national bodies. This coordinated action is centred on ensuring that organisations across the sector are implementing essential security requirements, including:

- ensuring that local Boards and their staff are taking the cyber threat seriously, understand the direct risks to frontline services and are working pro-actively to maximise their resilience and minimise impacts on patient care;

- following up the small number of critical CareCERT alerts within 48 hours to confirm that local organisations have taken necessary action, for example, have implemented security patches and updated their anti-virus software; and
- supporting local organisations to ensure they are identifying and moving away from, or actively managing, any unsupported systems by April 2018.

The plan set out in this document centres on ensuring local organisations are implementing the 10 data security standards supported by the CareCERT suite of national support services, and backed up by clear contractual obligations and by assurance and regulatory action.

We believe that the reviews and their recommendations will significantly contribute to enabling greater use of data in a safe, secure and legal way to benefit all of us.

Rt Hon Jeremy Hunt MP
Secretary of State for Health

Lord O'Shaughnessy
Parliamentary Under Secretary of State for Health

Executive Summary

Better use of information and data has the potential to transform health and care for everyone. However, organisations' resilience to cyber threats and the unimpeded, safe and secure flow of appropriate information and data across the health and social care system are critical to improving outcomes for all.

People must be confident that systems are secure and robust. Recent incidents, including the May 2017 ransomware attack, which affected many other countries' services as well as our own health and care system, have shown that the NHS can protect essential services in the face of a cyberattack, but they have also underlined the need for organisations to implement essential, strong data security standards.

People want to know that their privacy and rights are safeguarded, understand how and when information about them is shared, and, how and when they can make an informed choice about whether to share their data or not.

It was in this context, that the Secretary of State for Health commissioned a review on data security and data sharing in the health and social care system by Dame Fiona Caldicott, the National Data Guardian for Health and Care (NDG). In parallel, he commissioned a review by the Care Quality Commission (CQC), *Safe Data, Safe Care,* of current approaches to data security across the NHS. These focussed on strengthening data security across the health and social care system, and proposing a new model for data sharing.

Dame Fiona Caldicott's *Review of Data Security, Consent and Opt-Outs,* published on 6 July 2016, addressed these issues and considered two important aspects of people's trust:

- whether the IT systems that health and social care organisations use to deliver care and share information are secure and resilient to data security risks; and,
- how we can ensure that individuals are better informed about the basis upon which their information might appropriately be shared.

Following publication of these reviews, the Government undertook an extensive consultation, as the start of an ongoing dialogue with the public on these issues. The Government has taken into account the views expressed, and is pleased to confirm that it agrees with each of the NDG's and CQC's recommendations. These are set out in detail at Annexes A and B.

The Department of Health and its partners have made the following commitments to ensure the health and social care system in England realises the full benefits of sharing data in a safe, secure and legal way, and, that complements the existing Caldicott principles.

Case Study: **Alzheimer's Research UK**

Fred's Story

After losing his wife to Alzheimer's in 2010, 79-year old Fred decided to do something proactive to help research into the disease.

He played an online citizen science game developed by Deutsche Telekom and Alzheimer's Research UK called Sea Hero Quest, which collects anonymous information about a person's spatial navigation skills as they play. By choosing to share his data, Fred is one of 2 million people across the world helping scientists understand how spatial navigation changes with age, creating an important benchmark for future studies to improve the diagnosis of diseases like Alzheimer's.

Case study courtesy of Alzheimer's Research UK

We will protect information through system security and standards:

- The Government agrees to adopt and promote the 10 data security standards set out in this document, as proposed by the NDG's review.
- The Government also agrees to adopt the CQC's recommendations on data security.
- NHS Digital is working with the health and care community to redesign and update the Information Governance Toolkit to support and underpin the new standards. This will take account of the relative needs and expectations of different organisations when considering their data security capability.
- From September 2017, the CQC's well-led inspection framework will include the importance of meeting the data security standards. This will be supported by information from the redesigned Information Governance Toolkit.
- In summer 2017, NHS Improvement will publish a new 'statement of requirements' which will clarify required action for local organisations. Chief Executive Officers must respond to this with an annual 'statement of resilience', confirming essential action to ensure that standards are being implemented. This will include the requirement for each organisation to have a named executive Board member responsible for data and cyber security.
- To support implementation, we will take a targeted approach to communications and engagement for leaders and staff across the health and social care system, including with the primary care community, supported by guidance and a new staff training package.
- NHS Digital will build on its suite of advice and support services, called CareCERT, which forms part of the Data Security Centre, to support health and care organisations prepare their own resilience to cyber security threats, and to respond effectively and safely when they occur.

- We will boost investment in data and cyber security above the £50 million identified in the Spending Review to address key structural weaknesses, such as unsupported systems. We will target an initial £21 million of capital funding to increase the cyber resilience of major trauma sites as an immediate priority, and improve NHS Digital's national monitoring and response capabilities.

- NHS Digital will support the new data security standards and signpost health and care organisations to tools to identify potential vulnerabilities through the redesigned Information Governance Toolkit and the associated CareCERT suite of services. It will also help to identify organisations in need of additional support.

- We will work with a range of health and care organisations to assess whether other assurance frameworks such as Cyber Essentials Plus and ISO2700[1] meet their particular needs and through the Information Governance Toolkit to implement the data security standards.

- The NHS Standard Contract 2017/18 requires organisations to implement the NDG review recommendations on data security.

We will enable informed individual choice on opt-outs:

- We will support people to make informed choices about how their information is used and protected in the health and social care system.

- We will reinforce the importance of sharing information securely and appropriately for wider purposes, such as advancing medical science and protecting vulnerable people.

- By December 2018, people will be able to access a digital service to help them understand who has accessed their summary care record. By March 2020, people will be able to use online services to see how their personal confidential data[2] collected by NHS Digital has been used for purposes other than their direct care.

- NHS Digital will develop and implement a mechanism to de-identify data on collection from GP practices by September 2019.

- The National Information Board (NIB) will continue to focus on how to build greater public trust in data sharing for health and social care.

- We will give people the choice to opt out of sharing their data beyond their direct care, which will be applied across the health and social care system.

[1] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[2] The National Data Guardian's review used the term 'personal confidential data', which was also the term used in the second Caldicott report. The Government's response uses the same term for consistency, though we accept that there is a complex legal framework with the Data Protection Act and Common Law Duty of Confidentiality, which use different definitions as well as differing interpretations of these terms and that the commonly understood legal term is 'confidential patient information'. The Wellcome Trust's Understanding Patient Data initiative recognises the language used to describe patient data is complex and confusing. It is important that we use the right words to describe what we mean which are understandable and meaningful to people. Understanding Patient Data has suggested 'patient data' and 'patient health information' as the most effective terms to use. We will give further consideration to this issue as we implement the recommendations of the NDG review and in particular the new opt-out to ensure there is absolute clarity for the public.

- In moving to the national opt-out, we will honour existing type 1 opt-outs[3] until 2020 and consult with the NDG before confirming their removal.

We will apply meaningful sanctions against criminal and reckless behaviour:

- We will implement the UK data protection legislation in May 2018, which will provide a framework to protect personal data and will also impose more severe penalties for data breaches and reckless or deliberate misuse of information.

We will protect the public interest by ensuring legal best practice and oversight:

- We will put the National Data Guardian role and functions on a statutory footing.
- The Information Governance Alliance (IGA) will publish anonymisation guidance based on the Information Commissioner's Office (ICO) Code of Practice on Anonymisation in 2018.[4]
- We will clarify the legal framework by working with the Confidentiality Advisory Group (CAG) to ensure its approvals process under Section 251 of the NHS Act 2006 enables organisations to access the information they need, for example for invoice validation.

[3] Type 1 opt-out: The option for a patient to register an objection with their General Practitioner, to prevent their identifiable data being released outside of the GP practice for purposes beyond their direct care.

[4] Information Commissioner's Office, *Code of Practice on Anonymisation*, November 2012.

Case Study: **Alzheimer's Society**

Too high a price. How lack of data makes it harder to improve care.

By 2025 there will be 1 million people with dementia in the UK. At the moment there are significant gaps in the data available about dementia and, as a result, in our understanding of the quality of services people with dementia receive. Research by the Alzheimer's Society found that 47 per cent of carers felt that being in hospital had a significant negative effect on the general physical health of the person with dementia, which was not a direct result of the medical condition.

Freedom of Information requests showed that in 2015 the average length of stay for someone over 65 in hospital was 5.5 days, whereas for people with dementia it was 11.8 days. In the best performing hospitals, the length of time people with dementia stayed was the same or only marginally longer than the length of stay for people over 65 without dementia. However, in the three worst performing hospitals, people with dementia stayed between five and seven times as long as other people over 65.

This unacceptable variation is currently shielded from view because hospitals are not required to share this data publicly. It is therefore not clear where the problems exist or how they should be addressed.

The Alzheimer's Society is calling for hospitals to publish an annual statement of dementia care, including information on length of stay so that this can be routinely monitored. This will build-on recent developments that have placed more information and data on dementia in the public domain. This includes the Dementia Intelligence Network Fingertips tool and metrics that give an at-a-glance indication of how well services are performing on dementia care. Ultimately this will help identify areas where dementia care is inadequate and needs improvement and enable more targeted regulation of dementia services in hospitals.

> *"Whilst recent developments such as the Dementia Intelligence Network Fingertips tool place more information and data into the public domain, and the development of a dementia specific Clinical Services Quality Measure (CSQM) aims to provide an at-a-glance indication of how well services are performing, there are still wide gaps in the collection and availability of data that will help us not just to monitor and understand, but also take action to improve and develop the care and support that people with dementia are experiencing".*
> **Jeremy Hughes CBE, Chief Executive, Alzheimer's Society**

Case study included in the Richmond Group of Charities report: 'My Data, My Care', 2017

1. About the Consultation

1.1 In her *Review of Data Security, Consent and Opt-Outs*, the National Data Guardian for Health and Care (NDG) made it clear that further consultation and engagement should be a key priority for the Government. As a result, on the day that the Care Quality Commission (CQC) and NDG reviews were published, the Department of Health launched a consultation on the proposed data security standards and a new national opt-out.

1.2 The Government is grateful for all the responses to the consultation, which reflected the importance the public and many organisations attach to achieving a safe and secure system of data sharing in health and care.

1.3 The consultation on *New Data Security Standards and Opt-Out Model for Health and Social Care* took place over a two month period, beginning on 6 July 2016 and ending on 7 September 2016. The consultation document and feedback form were made available on the gov.uk website at https://consultations.dh.gov.uk/information/ndgreview-of-data-security-consent-and-opt-outs and a dedicated mailbox was set up to receive feedback directly.

1.4 In order to promote participation, approximately 500 professional and public stakeholders were directly engaged and signposted to the consultation exercise. The provision of supporting material helped guide discussion, enabling an informed response. This was supplemented by a range of digital promotional methods, including online discussion, employed to generate further awareness and interest. There were 638 responses to the consultation, most of which were submitted online.

1.5 We received responses from a broad range of organisations and individuals, including:

Members of the Public	Clinical Commissioning Groups
General Practice	Local Authorities
Arm's Length Bodies	Public Health Organisations
Social Care Providers	Commissioning Support Units
Government Departments	Special Interest Groups
Professional Organisations/ Associations	Hospital Trusts and Foundation Trusts
Research Bodies	Others

1.6 In addition to the formal online consultation, we held three events to engage with a wide range of people and explore the NDG review's findings in more depth. At each event, there was a session for professionals and a session for members of the public. The events took place in London, Southampton and Leeds and were attended by a total of 178 people comprising 111 professionals and 67 members of the public. Public representatives included people who use the health and social care system, and professional attendees included those working in direct care, information governance and information technology.

1.7 A summary analysis of consultation responses can be found at Annex F.

2. Data Security Standards

The health and social care system is being transformed by technology, bringing huge benefits to people and professionals, accelerating diagnosis and treatment, preventing ill-health, improving patient safety and leading to breakthroughs in research. With that comes a responsibility to keep both systems and data secure, which is vital to protecting the public, patients and service users, as well as maintaining their trust and confidence. The NDG's review found that risks to essential systems used to deliver care, or the loss of personal data undermine the public's trust. Data security incidents, such as the May 2017 global ransomware attack which affected NHS services, as well as other public services and private companies in many other countries, have highlighted the potential for cyber-attacks to disrupt services by having a direct impact on the availability of care for patients and service users.

The NDG's review recommended the introduction of 10 new data security standards[5], building on existing principles, to improve data security across the health and social care system. These were grouped under three leadership obligations: people, process and technology.

Throughout the consultation, we heard that there is strong support for the NDG's recommendations and 10 data security standards, but that strong Board level leadership and clear communication are required to enable organisations to implement these effectively.

In response and also in light of the recent attacks, the Government:

- **Accepts the NDG's 10 data security standards which have been strengthened to ensure organisations report incidents as soon as possible to the CareCERT service, and to ensure the Boards of local organisations are held to account for their implementation through strong regulation and assurance.**
- **Will boost investment in data and cyber security to address key structural weaknesses, such as unsupported systems, targeting an initial £21 million of capital funding to increase the cyber resilience of major trauma sites as an immediate priority.**
- **Will promote the CareCERT package of support services and training materials to help health and care organisations prepare their own resilience, and to help them manage incidents quickly and effectively when they occur.**
- **Will launch the redesigned Information Governance Toolkit in April 2018 to ensure that local organisations, as well as regulators, can be confident that the essential data security standards are being implemented across the sector.**

[5] See Annex D: The 10 Data Security Standards

Case Study: **British Orthopaedic Association and the National Joint Registry**

Using health information to monitor the performance of joint replacement surgery*

Many thousands of joint replacements take place in England every year. The National Joint Registry (NJR) links with Hospital Episode Statistics (HES) and NHS Patient Reported Outcome Measures (PROMs) data to give hospitals and surgeons feedback about their performance to help them review and improve patient care.

It is possible to compare performance across the country and identify patterns of failure rates with different implants, enabling surgeons to choose the most appropriate devices for patients, improving quality and reducing safety issues.

Data obtained from the NJR revealed that a particular brand of implant had high failure rates, resulting in the implant being withdrawn by the manufacturer. Without the NJR, this discovery might not have been as timely and beneficial to patient safety.

> *"I was really anxious before my hip replacement surgery, but having access to NJR data, online resources like the Public and Patient Guide and other patients' experiences was an enormous help. I learned more about my surgeon's practice, the hospital where my operation took place, and the replacement joint I received. This information made me feel better informed and involved. I was pleased to give consent for my record to be included in the NJR knowing that this could help other patients have successful surgeries, too. Thanks to this life-changing operation, I am now pain free and mobile for the first time in years."*
> **Sue Musson, hip replacement patient**

*This case study is supplied jointly by the British Orthopaedic Association (BOA) and the NJR, which is managed by the Healthcare Quality Improvement Partnership (HQIP). The BOA works with the NJR as a clinical partner, representing the views of the profession.

Case study courtesy of Association of Medical Research Charities:
'a matter of life and death: how your health information can make a difference', 2016.

A stronger approach: the data security standards

2.1 The data security standards[6], proposed by the NDG's review aim to minimise the potential for cyber and data security incidents to disrupt essential services, address the causes of paper-based and digital security breaches in the health and social care system, and help protect against future cyber and data risks. The standards were designed for the whole health and social care system and to be easy to understand. They recognise the value of safe, secure, appropriate and lawful sharing of data.

Broad support for the data security standards

2.2 The Government accepts in full the data security standards proposed by the NDG. Following discussion with the NDG we have strengthened Standard 6 (see paragraph 2.8). The Government also accepts the recommendations of the CQC's report *Safe Data, Safe Care.*[7] We are pleased with the positive response to the proposed data security standards that we heard through the consultation, from a broad range of organisations.

> *"An important step towards improving the robustness of data governance right across the health and social care system"*
>
> **The Wellcome Trust**

2.3 Better data security and the data security standards are critical to public trust in the use of data by the health and social care system.

> *"We consider that effective data security is essential if the public is to trust us to use data for public health analysis…"*
>
> **Health Statistics User Group**

2.4 The data security standards are designed to be fit for purpose now and in the future. The requirement to demonstrate compliance will be subject to ongoing review to keep in line with developments. Organisations will also be expected to understand and respond to changing and emerging threats.

2.5 As the NDG reflected, people are at the heart of improving data security; from day-to-day processes, through to leadership and senior ownership of risks. Data security is not just about improving technology or repelling sophisticated cyber-attacks. The processes for accessing and using systems and data – both electronic and paper based – must be robust, secure and designed with end users in mind.

2.6 The Department of Health is working closely with health and care organisations, and security agencies, to understand and mitigate the cyber and data security risks to the health and social care system. A coordinated programme will raise awareness at all levels, ensuring Board level ownership to support the vital action needed to mitigate risks in each organisation.

2.7 The Department of Health is working closely with the National Cyber Security Centre (NCSC) to understand cyber security risks and how they relate to health and care. Key national partners including NHS Digital, NHS England and CQC are helping to ensure that we are agile in adapting to the evolving cyber security landscape. The Department of Health is also working across Government to ensure the health and social care system benefits

[6] See Annex D: The 10 Data Security Standards

[7] The Care Quality Commission, *Safe Data, Safe Care,* July 2016

Case Study: Macmillan Cancer Support

Caring for people after diagnosis

Macmillan's use of data to improve care for people living with and beyond colorectal cancer in Sheffield

Macmillan and a partnership of Clinical Commissioning Groups in South Yorkshire and Bassetlaw entered into a 'Survivorship Partnership' to improve the experience and outcomes of local people living with and beyond colorectal cancer. They developed and tested a new model for aftercare, moving people from a one size fits all approach directed by the health and social care system to one that offers more options for a self managed approach.

To understand the use of the local health service and population needs, Macmillan worked with a partner to link and analyse anonymised healthcare data to track use of hospital services. This work helped identify the different health outcomes and cancer journeys people with colorectal cancer could experience.

Once these different journeys and health outcomes were identified, Macmillan was able to design and test new ways of helping people with colorectal cancer through the often complicated care pathway and help them look after themselves better.

Comprehensive, routinely collected data provided a high level view of a large number of people, enabling a cost and population analysis to be carried out.

The data was used to model and design new pathways of care that better meet people's needs and make efficient use of resources. Without this linked local data, local clinicians would not have been able to see how people with colorectal cancer were using their services, how they were doing and where targeted improvements might make a difference. The new care pathways have been implemented and are currently being tested.

Case study included in the Richmond Group of Charities Report: 'My Data, My Care', 2017

from the National Cyber Security Strategy, as part of the vision that the UK is secure and resilient to cyber threats, prosperous and confident in the digital world.

2.8 Learning from previous events, early involvement by CareCERT is clearly central to the successful management of a data security incident. For this reason, we have strengthened Data Security Standard 6[8] which now requires significant cyber-attacks to be reported by health and care organisations to CareCERT as soon as possible following detection.

2.9 We will produce materials, measures and metrics to support local implementation of the standards and to underpin the redesigned Information Governance Toolkit. These materials will also support organisations to meet the requirements of the NHS Standard Contract. In the consultation, health and care organisations asked for more information on how the standards will be applied in practice, so we will also implement a range of initiatives to support organisations to embed the standards.

[8] Data Security Standard 6: Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken as soon as possible following a data breach or near miss, with a report made to senior management within 12 hours of detection. Significant cyber-attacks are to be reported to CareCERT immediately following detection.

Learning from the May 2017 ransomware attack

2.10 The WannaCry cyber incident in May 2017 was the largest ransomware incident observed to date, affecting services in many other countries, as well as the NHS in the United Kingdom. This attack reaffirmed the potential for cyber incidents to impact directly on frontline care. Following this incident, Will Smart, the Chief Information Officer (CIO) of the health and social care system has started a lessons learned review, to report in October 2017 and inform further action.

2.11 Immediate lessons have already been identified from the recent incident, including:

- The need to ensure organisations implement critical CareCERT alerts, including software patches, and keep anti-virus software up to date; NHS England and NHS Improvement are already following up the small number of critical CareCERT alerts within 48 hours to confirm that local organisations have taken necessary action – starting now with major trauma units and Ambulance Trusts, and rolling out more widely in summer 2017.
- The need for organisations to identify and prioritise action to move away from or isolate unsupported systems; local organisations should be aiming to have isolated, moved away from, or be actively managing any unsupported systems by April 2018.
- Ensuring that organisations, their Boards and their staff, are taking the cyber threat seriously, understand the direct risks to front line services and are working pro-actively to maximise their resilience and minimise impacts on patient care. The plan set out below, centres on ensuring local organisations are implementing the 10 data security standards supported by the CareCERT suite of national support services, and backed up by clear contractual obligations and by assurance and regulatory action.

2.12 Boosting cyber resilience and improving the response to cyber incidents remains an urgent priority. The Government's priorities for action, already being taken forward by the Department of Health and central bodies, are set out below and summarised in Annex G, focussing action on:

- Establishing a clear contractual and regulatory framework.
- Addressing infrastructure weaknesses.
- Communications, engagement and training, to staff and leaders in the system.
- Building local performance and boosting capability.
- Improving threat surveillance and incident response.

A culture of security

2.13 Alongside examples of best practice, many consultation responses highlighted inconsistent levels of data security across the health and social care system. We do not underestimate the importance and challenge of bringing every organisation across health and care to an appropriate standard of data security. The 10 data security standards provide the basis for achieving this goal. We will work with others across the system to ensure every organisation has data security measures in place which are proportionate to the risks they face.

2.14 We heard through the consultation that clear communications are needed to support staff and leaders to understand their responsibilities towards data management.

> *"The key issue is to ensure that staff are able to understand, and recognise the importance of, the basic principles in line with their role and are therefore adequately prepared to apply their knowledge to different scenarios in their daily working routines"*
>
> **The British Medical Association**

2.15 Implementing the 10 data security standards and building organisational resilience will require bringing together local cyber security and information governance expertise into coordinated information assurance activity. In that context, and in line with the NDG's recommendations that the current Information Governance Toolkit should be redesigned, NHS Digital is working to replace it with a new framework by April 2018, to support organisations in improving their own levels of data security.

2.16 The review set out that leaders, particularly at Board level, will be key to ensuring that standards are embedded at a local level. Many of the consultation responses highlighted a similar theme, acknowledging that the necessary culture change will depend on effective leadership.

> *"It does need leadership throughout an organisation to ensure that these standards are given a high profile and endorsed and supported to ensure that all staff understand and can meet their obligations for data security"*
>
> **Response from individual**

2.17 Data security simply will not improve across the health and social care system without strong Board level leadership which views and prioritises data security as importantly as financial integrity and clinical safety. The standards backed up by a clear contractual and regulatory framework, make clear that Boards must take responsibility for their organisation's data security risks, as experience has shown that Board ownership and leadership are critical to an organisation effectively responding to data security incidents. Ensuring that local Boards are implementing the 10 data security standards will be a factor considered by CQC and NHS Improvement in decisions to apply their regulatory powers. This will include the requirement for each organisation to have a named executive Board member responsible for data and cyber security.

2.18 Clear communication is crucial to changing behaviours and culture. Working with NHS Digital and NHS England, the Department of Health will take a targeted approach to communications designed for leaders and staff across the health and social care system. For leaders, our messaging will concentrate on the need for them to understand, regularly assess and manage their organisation's data and cyber risks. For staff, messaging will focus on simple steps that they can take on a day-to-day basis to be more cyber resilient. Throughout, we will stress that keeping data safe and secure is inseparable from good patient care and builds and maintains public trust. This will be supported by a new staff training package.

2.19 Whilst the existing community of information technology and information governance experts will play a vital role in supporting their organisations in making these cultural changes, they alone cannot make the required improvements in data security. To make meaningful improvements, it is critical that leaders and staff across the system take ownership of it as an integral part of what they do.

Case Study: Asthma UK

Using health information to manage chronic conditions

5.4 million people in the UK are currently receiving treatment for asthma. The UK has some of the highest prevalence rates in Western Europe and on average 3 people a day die from asthma. Despite this, one in two people do not have their asthma well controlled.

In 2015, Asthma UK began working with a range of partners from across Europe on a three-year study to develop a novel sensor-based inhaler, myAirCoach, which connects to a patient's smart device and monitors a range of physiological, behavioural and environmental factors. It aims to help asthma patients to self-manage and increase their awareness of their condition. It will also create a new and more comprehensive dataset of the biological state of people's asthma on a day-to-day basis. This can then be examined by researchers aiming to discover if asthma exacerbations can be predicted and treated at an earlier stage. The project will build evidence about the potential for mobile health to manage asthma and other long-term conditions.

"MyAirCoach is a ground-breaking project that will pave the way for more effective management of asthma based on real-time data from the patient and their environment. The use of a wide array of information will help to predict a worsening in asthma symptoms, such that treatment can be subsequently adjusted to avert a life-threatening asthma attack." **Researcher perspective**

Case study courtesy of the Association of Medical Research Charities: 'a matter of life and death: how your health information can make a difference', 2016

Resources and implementation

2.20 We heard from respondents about the various challenges they face which could impact their implementation of the data security standards, especially for smaller organisations (and particularly in social care, primary care and the voluntary sector).

2.21 The Government fully appreciates the need to balance increasing data security against disproportionate financial and resource burden. For example, a small care home without digital care records would be expected to take different steps compared to a large hospital that digitises records at the point of care.

2.22 Small changes can make big differences. Simple changes involving people and processes are often more effective than implementing expensive technological solutions; high-value rather than high cost interventions. We are aware of incidents where cyber-attacks have exploited basic vulnerabilities that could have been avoided by regularly reviewing existing firewall rules and password management practices, actions costing very little, but requiring vigilance, education and commitment.

2.23 Implementing CareCERT and the redesigned Information Governance Toolkit will encourage and enable organisations to take steps that are simple, sensible, and consider the real world consequences of cyber security rules, including the impact on staff time. The redesigned Information Governance Toolkit's requirements will be proportionate to the risk profile of organisations. We will work with the Local Government Association (LGA) and Association of Directors of Adult Social Services (ADASS), the primary care community, social care and voluntary, community and social enterprise sectors to ensure that there is also a proportionate expectation of social care organisations and that appropriate support is available.

2.24 We also heard from the primary care community that there are specific challenges to implementing the data security standards in these settings. We recognise that GPs in particular are dependent on Clinical Commissioning Groups (CCGs) and the GP systems suppliers for their IT provision. We will work with the GP systems suppliers to make sure the technology used in general practice is secure by default, and we will work with the primary care community to ensure that data security training meets its specific needs.

Technology

2.25 The consultation responses identified that implementation of the data security standards might also be impacted by the quality of an organisation's existing systems. We are aware that it is not always possible or desirable to update systems, particularly in the case of clinical hardware. Nevertheless, unsupported software and ageing technology represent a significant cyber risk, as they are not subject to the latest security patches and updates released by manufacturers.

> *"Many health and care organisations rely on systems that are based on older operating systems and software, which may be unsupported. In many instances, the replacement of these systems and software may be impracticable or very costly, at least in the short term"*
>
> **Public Health England**

2.26 Data Security Standard 8[9] responds to the need that the NDG and CQC reviews identified to remove unsupported systems and software. Work is underway to determine the fastest and most cost effective way to move the NHS off unsupported operating systems. NHS Digital is publishing technical advice and guidance in July 2017 to identify such systems and to support organisations to understand and actively manage their risk. We will focus on reducing the use of unsupported platforms and browsers, targeting an initial £21 million of capital funding to increase the cyber resilience of major trauma sites as an immediate priority. Local organisations should be aiming to have isolated, moved away from or be actively managing any unsupported systems by April 2018.

[9] Data Security Standard 8: No unsupported operating systems, software or internet browsers are used within the IT estate.

Case Study: Stroke Association

Supporting healthcare professionals to raise standards – targeted information offer on atrial fibrillation

Atrial fibrillation (AF) is a type of irregular heartbeat which can lead to blood clots causing a stroke. AF contributes to 20 per cent of strokes in England, Wales and Northern Ireland, yet it is estimated that over a third of people with AF do not know they have it. If the 1.4 million people with AF in England were identified and treated with a medicine to prevent blood clots, around 7,000 strokes could be prevented and around 2,100 lives saved every year. Unfortunately, not only is AF often undetected, but improved guidance on how to manage it effectively could be more effectively implemented.

Data shows that 31 per cent of eligible people with AF are not being given treatment to prevent blood clots despite guidance. The Stroke Association worked with Public Health England, the Royal College of GPs and the Royal College of Physicians to understand where and how AF management could be improved. Together they created 'AF: How can we do better?' a free information document showing how each Clinical Commissioning Group (CCG) is performing. This has been used to make a strong case to CCGs to improve AF care.

Data enabled the Stroke Association and partners to identify how many people should have been receiving treatment that could reduce their risk of stroke but were not. The Stroke Association and partners used this knowledge to highlight the issue and take action, helping ensure people with AF are identified and given access to treatments; ultimately preventing strokes and saving lives.

"(When) I received the 'AF: How can we do better' data... we were building a case for improving AF detection and treatment in order to reduce the rates of preventable strokes in people with AF. I was able to use the data to evidence the case for change in Hounslow and to engage partners in the work. I am now working in collaboration with other professionals to run a pilot project to improve the detection of people with AF in Hounslow"

Dr Sadia Khan, Consultant Cardiologist at Chelsea and Westminster NHS Foundation Trust

Case study included in the Richmond Group of Charities Report: 'My Data, My Care', 2017

2.27 NHS Digital will enhance the CareCERT suite of services to further support health and care organisations to tackle the greatest technological risks to data security, working to help identify local threats and vulnerabilities and mitigating them before they become incidents. NHS Digital will work with the Global Digital Exemplars – NHS providers that deliver exceptional care through the world-class use of digital technology and information – to provide peer support to health and care organisations that need to identify and plan to migrate away from unsupported technology.

2.28 We are working in partnership with Microsoft to help mitigate the immediate risks associated with unsupported software.

2.29 Central support for NHS Digital's national applications operating on outdated platforms will be phased out, with Windows XP support being withdrawn from 2018. The Department of Health will work with partners to negotiate a centrally managed agreement with software providers to provide a common core build of an up-to-date operating system for health and care. We will boost investment in data and cyber security above the £50 million identified in the Spending Review to address key structural weaknesses, such as unsupported systems, and increase NHS Digital's national monitoring and response capabilities.

2.30 Emails sent to and from NHSmail accounts or to other secure email systems are protected to UK Government standards. This ensures that sensitive and confidential information is kept safe. Any health or care organisation wishing to operate its own email systems securely and connect them to other secure email services such as NHSmail must meet the requirements stated in the secure email specification.

2.31 Increasingly, systems will be secure by default rather than security being an afterthought, through work to ensure that the systems commonly used by the health and social care system have in-built security.

Training

2.32 NHS Digital has worked with Health Education England (HEE) to develop a new staff training package which will replace existing training. The training is being designed to help staff across health and social care to understand their responsibilities for keeping and sharing data securely and the surrounding legal framework.

2.33 We heard from the consultation that there were concerns about what would happen to staff who 'failed' the mandatory training. People also wanted to understand how the requirement to train 'all' staff would be assessed in practice. As with the current Information Governance Toolkit, organisations will need to demonstrate that staff accessing and managing personal confidential data have successfully completed data security training. By replacing existing training we aim to prevent extra burdens being placed on staff. Where staff do not pass mandatory training, we would expect their employing organisation to support them in understanding their responsibilities for data security and for handling personal data.

CareCERT

2.34 Through the consultation we heard that individual organisations often did not feel they had the data and cyber security expertise required to make informed decisions about improving their cyber security or to respond to incidents.

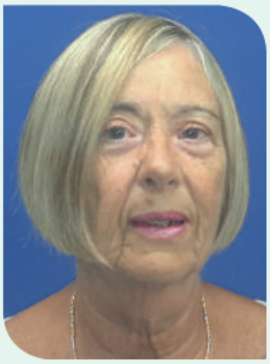
> *"Lack of IT/Cyber Security specialists within organisations may be a significant barrier. Specific consideration should be given to how to increase the availability of these experts."*
>
> **NHS England**

2.35 Providing national support to organisations will be vital to supporting the health and social care system, as a whole, to be resilient to data security risks. This will be delivered through NHS Digital's CareCERT service which consists of four core strands:

- **CareCERT Intelligence** actively monitors health and care networks to analyse threats and broadcast alerts to support those running health and care IT systems to defend against the latest risks.

Case Study: Multiple Sclerosis (MS) Society

The UK MS Register



"Working on this project is my way of contributing to scientific research. The UK MS Register is increasing our understanding of the experiences of people living with MS in the UK, allowing the MS Society to focus campaigns on difficult issues and identify new research priorities."
Val Gouby, MS Society Research Network member

There are around 100,000 people living with MS in the UK, but we have a relatively poor understanding of the condition. For example, the exact number of people diagnosed, how their MS is affecting them, how they manage and deal with their condition, whether they are in employment and how the available treatment affects their long term health. This information is vital to develop and understand the effects of new treatments, develop management techniques and provide better services.

The MS Register currently has 15,232 individuals with MS providing information. The Register combines health records from the NHS with information provided directly by people living with MS. By gathering, linking and analysing this data, the Register allows researchers to gain important new insights into the lives of people with this condition.

Some people taking part in the Register have reported, for example, that they tend to have high levels of anxiety and depression. Further research into this found a reported high level of anxiety in women and high level of depression in men. Findings like this allow the major UK charity supporting people with MS, the MS Society, to focus campaigns on the issues that matter most to people living with the condition. The more data the Register can gather, the more the researchers hope to learn.

Case study courtesy of Understanding Patient Data.

- **CareCERT React** will provide a hotline for dealing with cyber security incidents when they happen, providing first-line support and detailed guidance on mitigating threats.
- **CareCERT Knowledge** will share best practice and be a repository of knowledge for health and care organisations looking to improve their level of cyber security.
- **CareCERT** also includes a support package enabling organisations to undertake an on-site assessment of their cyber security capability relative to the level of risk they face. This will allow them to take actions in response to these findings to mitigate and reduce their cyber risk. 60 NHS Trusts and Foundation Trusts have already undergone an on-site assessment, and more organisations will be assessed this year prioritising those organisations affected by the ransomware incident in May.

2.36 Some organisations are already using CareCERT services to improve their level of data security.

> *"The Trust has membership of CareCERT and specialist software is in place and regular ongoing monitoring of cyber threats are completed with reporting being established via the Information Governance Group and the ITC Senior Managers group."*
>
> **Coventry and Warwickshire Partnership NHS Trust**

2.37 In combination with our national initiatives to reduce technology-based risk and foster a culture of data security, CareCERT will help us to work across the health and social care system to support organisations, individually and collectively, to increase their levels of data security.

2.38 Alongside its on-site assessment programme, NHS Digital will establish a process of unannounced spot checks, to help support local organisations' own work in identifying vulnerabilities and prioritising local actions to mitigate them.

Increasing digital and information assurance

2.39 We heard a clear case for changing the current assurance frameworks around data security. In particular, completing the current Information Governance Toolkit can be burdensome and is often considered a 'tick-box' exercise.

> *"We also welcome the recommendations made by [the Review] for supporting practices in implementing the new standards and ensuring they are adhered to, including that 'the Information Governance Toolkit (IGT) should be redesigned around the new standards"*
>
> **The Royal College of General Practitioners**

2.40 While there was some support for CQC's inspection regime to cover assurance of data security we also heard concerns about whether CQC had the capability or capacity for this task.

2.41 The redesigned Information Governance Toolkit will measure the extent to which individual organisations have embedded the data security standards and use this as part of a scorecard to assess organisational 'cyber capability'. This approach will provide individual organisations with the necessary tools to assess their own adherence to the standards and level of cyber capability, as well as providing a national picture of data security across the health and social care system, and intelligence for independent assurance processes. To ensure that the standards are being prioritised and implemented, in summer 2017, NHS Improvement will publish a new 'statement of requirements' which will clarify required action for local organisations, which Chief Executive Officers must respond to with an annual 'statement of resilience', confirming essential action has been taken. This will include the requirement for each organisation to have a named executive Board member responsible for data and cyber security.

2.42 In light of the findings of the CQC's report *Safe Data, Safe Care,* and the NDG's recommendations, the Government believes that data and cyber security should form part of CQC's well-led inspection framework. However, the role of CQC does not include acquiring cyber security expertise to assess the implementation of data security measures. A number of consultation responses expressed concerns as to whether it would be appropriate for CQC to assume such a role.

2.43 From September 2017, data security will form part of the CQC's role in assessing how well-led NHS Trusts are. GPs and adult social care providers will follow from November 2017, with CQC's inspection framework to be further developed by April 2018 as the other measures described in this response are being rolled out. The Government also encourages CQC to use its visits to assess that health and care providers have organisational processes in place to effectively manage their data and cyber security risks, in the same way that providers would audit and validate financial integrity and patient safety. Assessment of the data and cyber security measures themselves will be done through other assurance frameworks including the redesigned Information Governance Toolkit and the wider CareCERT suite of tools.

2.44 In addition to CQC's important role, the Department of Health will have a role in ensuring that our key national partners and the wider health and social care system work together effectively to mitigate the sector's security risks.

2.45 As one specific example, it is vital that local organisations are implementing CareCERT cyber security alerts. NHS England and NHS Improvement are already following up the small number of critical CareCERT alerts within 48 hours to confirm that local organisations have put necessary plans in place – starting now with major trauma units and Ambulance Trusts, and rolling out more widely in summer 2017.

3. Data Sharing and Opt-Outs

Sharing information has immense potential to improve the health and social care system, as well as improving outcomes for individuals. Building public trust, awareness and understanding in the use of patient information is key to unlocking the potential benefits that this information can bring. This trust is dependent on the public knowing how and why their information is used and what choices they have.

In her review, the NDG reflected on the vital importance of using and sharing information for public benefit, whilst emphasising that public trust is the foundation for this to succeed. The review included a new 8 point opt-out model[10] building on existing data sharing principles and good practice.

The consultation demonstrated that this message broadly resonates with public and professionals alike. In general, there is warm support for the NDG's recommendations on information sharing and the proposed national opt-out.

Alongside this overall support, the key message from both the NDG review and the consultation was that we need to take the time to get this right, and that a great deal of careful work and testing will be needed to implement the new national opt-out.

The Government accepts the NDG's recommendations on information sharing in health and social care.

To deliver the recommendations, we will:

- **Ensure that the national opt-out is implemented effectively from March 2018, engaging the public to understand what their data is used for and by whom, and the choices that they can make around that use.**
- **Ensure that the NHS and social care manages the transition to the national opt-out effectively by 2020.**
- **Support professionals to implement the national opt-out successfully.**
- **Support legislation to put the role of the NDG on a statutory footing.**
- **Implement stronger measures to protect personal data, through UK data protection legislation to introduce more severe penalties for data breaches and to deter reckless or deliberate misuse of information from May 2018.**
- **Work with other stakeholders, including Understanding Patient Data, to develop communication tools to explain effectively to the public, data and information sharing in health and care.**
- **Ensure that NHS Digital implements a tool to enable patients to access and understand how their data has been used nationally by March 2020.**

[10] See Annex E: The National Data Guardian's Eight Point Model

Case Study: Jessica's Story

100,000 Genomes Project

The world leading 100,000 Genomes Project is already providing answers and changing lives.

Jessica, aged 4, had a rare, undiagnosed genetic condition when she joined the project. She had previously found herself on a "diagnostic odyssey" involving serial referrals to several specialists and a plethora of, often invasive, tests. Taking part in the project meant that whole genome sequencing pinpointed the underlying genetic changes responsible for her condition and she now has a diagnosis.

Since her diagnosis, her family have been able to make positive changes for Jessica, including to her diet, which means her medication dose may be reduced and her epilepsy may be more easily controlled.

The project is building a unique dataset which links genomic and medical data. Researchers will analyse this with a view to making new scientific discoveries and medical insights which will help more patients like Jessica.

Image courtesy of Great Ormond Street Hospital

A trusted system

3.1 Sharing information and data offers immense potential to improve the NHS and social care system, unlock new treatments and medical breakthroughs, and improve our and others' lives. But these benefits rely on patients and the public having the confidence for their data and information to support the NHS, knowing that the use of their data is appropriate and legal, and that their data is held securely.

3.2. The storage and use of health and social care data is protected in a number of ways, in particular the Common Law Duty of Confidentiality and Data Protection Act (1998), soon to be replaced by new UK data protection legislation, which provide the legal framework for the processing of all personal data, other specific legislation such as the Control of Patient Information Regulations (2002), as well as non-legislative measures such as the Caldicott principles. There are some circumstances where opt-outs do not apply, for example where there is a legal requirement to share data.

3.3 The Secretary of State for Health established the National Data Guardian for Health and Care in November 2014 as the authoritative voice of patients and service users in terms of how their health and adult social care data is used.

3.4 To strengthen and formalise this role further and to create Parliamentary accountability, we are working to put the NDG on a statutory footing.

3.5 In addition to the existing Caldicott principles, the data security standards and the national opt-out will enable individuals to make choices about sharing their data and information, within a safe, lawful, secure environment across the health and social care system.

3.6 To help build trust, we will publish a pledge to the public to uphold the principles of the NDG review regarding how their data will and will not be used and their choices in this.

Implementing a simplified national opt-out

3.7 The NDG review recognised that the current range of opt-outs is confusing and that people want a simplified national opt-out which makes it clear to everyone when data about individuals will be used and in what circumstances they can opt out. In general, people were content with their data being used for the care that they received, and with anonymised information being shared for purposes beyond their direct care.

3.8 The NDG review reflected on the public's expectation that their data was already being shared for their direct care. The duty to share information can be as important as the duty to protect patient confidentiality.[11] The public, health and care professionals and organisations need clarity regarding how data can be shared lawfully and securely for those purposes. We will commission NHS Digital and NHS England to develop a framework (to be agreed with the NDG, Department of Health and the ICO) to support the system in sharing data for direct care and safeguarding children and adults by July 2017.

3.9 During the consultation we heard about the public's expectation that information about their choice is clear, easily available and accessible, and that the corresponding opt-out to share patient data beyond direct care is simple, easy to find and easy to use. We also heard that those who have already expressed an opt-out were keen to know how their wishes will be respected. The GP community also stressed the importance of maintaining people's trust in their healthcare professionals to look after their information safely and respecting their wishes for how it is used.

3.10 The NDG recommended a new opt-out to give people a clear choice about how their personal confidential data is used for purposes beyond their direct care. We endorse the NDG's proposed national opt-out and intend to implement it, whilst taking the time needed to get it right. The new opt-out will clarify how people can opt out, recognising that information will flow where there is a mandatory legal requirement, an overriding public interest or other exceptional cases. Individuals will be able to make their choice known online as well as in person.

[11] Caldicott Principle 7 – The duty to share information can be as important as the duty to protect patient confidentiality. Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

Case Study: Derby City Council

Sharing information to improve health and care

People who have a fall at home often have to access emergency services and residential care. This can have a lasting impact on their health and wellbeing. Health and care organisations wanted to support people more at home wherever possible by redesigning and improving the services provided, and the effectiveness of those services.

The organisations did not need to know the names and details of every patient who had previously had a fall but they did want a better understanding of the characteristics of those patients as well as the services they had accessed before and after the fall to ensure that local commissioned services were delivering value for money and linking effectively with other services.

By linking health and care information, the organisations were able to analyse key traits of the at risk population. When services commissioned to treat fallers were established, they were able to evaluate their success by comparing the outcomes of those people who had received them with those who had not.

Case study courtesy of Derby City Council and the Local Government Association

People will be able to express their own preference on sharing their data and be able to change their preference. Where someone has opted out, this will be respected by all health and care organisations. During 2017, we are working collaboratively with stakeholders and the public to test how the opt-out can be presented in a meaningful way.

3.11 The Government agrees with the NDG's proposal that existing opt-out arrangements should be improved, whilst recognising that careful consideration should be given to managing the existing opt-outs.

For patients who have registered an existing type 1 opt-out[12], we will honour these until 2020 to allow the new national opt-out to be implemented, and for full engagement with primary care professionals and the public. We will consult the NDG before confirming the removal of type 1 opt-outs. We will keep the level of opt-outs under review to ensure that there is no negative impact on patient safety and care and will seek advice from the NDG if this occurs. We will also work with the NHS and stakeholders to transition type 2 opt-outs and communicate the agreed approach with people who have expressed a type 2 opt-out in the existing system.[13]

[12] Type 1 opt-out: The option for a patient to register an objection with their General Practitioner, to prevent their identifiable data being released outside of the GP practice for purposes beyond their direct care.

[13] Type 2 opt-out: The option for a patient to register with their General Practitioner, to prevent their identifiable data leaving the Health and Social Care Information Centre (now NHS Digital) in an identifiable form. This applies to personal confidential data received by NHS Digital from all sources, not just from General Practitioners.

3.12 During this period, we will work with GP professional associations and GP systems suppliers to explore options for further improvements, for example to de-identify patient data on collection from the GP surgery.

3.13 The new national opt-out is a significant step forward in allowing people to more easily state their preference about the use of their health and care information. It will provide a single and simple mechanism for individuals to opt-out of their data being shared beyond their direct care.

Transparency

3.14 Providing the national opt-out is just one way in which we are personalising health and care, and empowering patients to have more control. We aim to ensure that patients have a meaningful choice about how their data is used, for research and for the wider NHS, supported by greater transparency so that they can see why and how their data is accessed, by whom, and the benefits this has.

3.15 As the statutory safe haven for collecting, storing and analysing health and care information, NHS Digital already publishes a register which sets out what data has been released, to whom, why and the intended benefits for doing so. This means that individuals can see what information organisations hold about them. By December 2018, people will be able to access a digital service to see who has accessed their summary care record, building on existing services offered by some companies which enable people to see who has accessed their electronic patient record. By March 2020, supported by developments in technology, people will be able to use online services to see more clearly how their data collected by NHS Digital has been used for purposes other than their direct care. We will also continue to challenge other parts of the health and social care system to improve transparency and enable people to see how their data is used.

3.16 The NDG review also gave some examples where the national opt-out should not apply. The review looked in particular at invoice validation for services that are not covered by a contract. For example, when receiving NHS-funded care, in a different part of the UK from where they live, a patient's identifiable data would be needed so that the provider could be paid for their services, despite not having a contract with that patient's commissioner.

3.17 Without having access to all patients' data, including those who have opted out, commissioners could not then validate the invoices for the services delivered to those people. Providers would not be fully reimbursed for the services they provide to patients, and commissioners would not be able to account for all the public money they are responsible for. NHS England estimates that hundreds of thousands of non-contracted activity invoices are processed by CCGs every year, worth an annual total of up to £1 billion. Applying an opt-out in this instance would represent a serious financial risk and pose an unacceptable barrier to the fair and efficient running of health services.

3.18 The existing Regulations under section 251 of the NHS Act 2006 already enable confidential patient information to be shared for invoice validation, when approved by the Secretary of State for Health, following advice from the Confidentiality Advisory Group (CAG). Rather than making new section 251 Regulations to authorise invoice validation (which would not be legally necessary), the existing Regulations can continue to be used, but the CAG advice and Secretary of State for Health approval should clarify that the

Case Study: Kidney Research UK

Using patient data to measure quality and drive change in renal services

In the UK over 3,700 people a year die while on dialysis and more than 250 people die while waiting for a kidney transplant around 5 people every week.

Researchers linked patient data from the UK Renal Registry with Hospital Episode Statistics data to understand why people on dialysis were going to hospital.

They found that hospital admissions were 69 per cent higher, and deaths were 33 per cent higher, in patients who had a two day break in their dialysis treatment. Patients receiving renal replacement therapy (dialysis or a transplant) in some centres were 4 times more likely to be admitted than similar patients treated in other centres.

This has important implications for how services and clinical pathways are designed. Health services can now take action to plan dialysis services to reduce the risk of health complications or even death.

> *"As a person living with kidney disease, it's important for me to see that understanding about treatment is moving forward. That's why it is so important that the Renal Registry has access to this data I feel really strongly about this."* **Patient perspective**

Case study courtesy of the Association of Medical Research Charities: 'a matter of life and death: how your health information can make a difference', 2016.

opt-out should not be applied with regard to invoice validation. More generally, we will work with CAG to agree a shorter and less burdensome process for specific information flows which are ongoing and longer term, whilst retaining key safeguards. We will work with the NDG and other key organisations such as NHS England to develop and implement these proposals.

3.19 The NDG review also set out some examples where the opt-out would not apply as sharing data in certain circumstances is required by law or court order. For example, the CQC has powers to require documents, information and records for their inspection purposes so that they can ensure health services are safe and high quality and the NHS counter fraud service – NHS Protect – has powers to prevent, detect and prosecute fraud in the NHS. Information must also be shared for child safeguarding purposes and health professionals are required to report known cases of female genital mutilation to the police.

Testing the new national opt-out

3.20 The new national opt-out will be robustly tested and developed collaboratively with the public and professionals.

3.21 During the consultation we heard that there is a public expectation that information about their choice is clear, easily available and accessible, and that the corresponding opt-out itself is simple, easy to find, easy to understand and easy to use. This feedback reinforces the principles behind the new national opt-out recommended by the NDG.

> *"AMRC would advise that further user testing is undertaken to ensure the language of the consent/opt-out question supports public understanding. The consent/opt-out model and related information must take into account social, cultural and educational differences in the population"*
>
> **Association of Medical Research Charities**

3.22 To ensure that making a decision on the sharing of one's data is both understandable and easy, further testing will be conducted to inform how the national opt-out is implemented and what support and information people need in order to make an informed choice.

3.23 The Wellcome Trust's engagement initiative on data sharing 'Understanding Patient Data' has tested the words used when talking about data and information sharing across the health and social care system in order to develop clear and understandable terminology. This has been helpful and will inform future communications and engagement.

Sharing anonymised information

3.24 There is a strong consensus that sharing data can improve outcomes and support the delivery of high quality health and care services. Very often these benefits can be realised without using identifiable data. Organisations should be mindful of the Caldicott principles[14] that only relevant information about a patient should be shared between health and care professionals in support of the individual's care or wellbeing. For purposes other than direct care, where possible, anonymised data should be used in accordance with the ICO's guidelines. As the NDG set out, this principle needs to be consistently promoted and applied across the health and social care system.

3.25 Through the consultation, we heard compelling reasons about why the opt-out should not be applied to anonymised information, alongside the need to be clear about what is meant by 'anonymised' and a call for assurance about how that data would be protected.

[14] Principle 2. Don't use personal confidential data unless it is absolutely necessary - Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
Principle 3. Use the minimum necessary personal confidential data - Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.

Case Study: **Salford Lung Study**

"Patients don't really feel as if they're in a study so they behave as they normally would, and we can get a better idea of how treatments work in the real world."
Professor John New
Consultant Physician Salford Royal
& NWEH Chief Clinical Officer

In the UK, Chronic Obstructive Pulmonary Disease (COPD) affects around 1.2 million people, so improving available treatments is important. Clinical trials of new treatments have strict rules that exclude a large number of patients, for example those with other conditions such as diabetes or heart disease. The Salford Lung Study (SLS) was designed to include patients who would often be excluded from a traditional clinical trial. It is pioneering a new way of conducting clinical trials that could give doctors and researchers a better idea of what happens when a new medicine is used in the 'real world'.

The SLS looked at the safety and effectiveness of a new treatment for COPD. This collaborative study was placed in Salford because they already had integrated electronic healthcare records. The study relied on the Linked Database System (LDS) developed by NorthWest EHealth (NWEH) and securely hosted within the NHS network, which linked together the data of consenting patients across all of their everyday interactions with their GPs, pharmacists and hospitals. This allowed the researchers to get a much more accurate sense of the impact of the treatment, for more typical people with COPD, than they would have had through the traditional clinical trial environment.

By linking together electronic healthcare records from different sources across the NHS it was possible to track over 2,800 patients over a 12 month period. By collecting healthcare information both quickly and efficiently, in line with best practice guidelines for security of patient data, the NWEH system offers responsiveness to patient safety, high quality data and shorter timelines for studies. The initial results from this trial have shown that patients significantly benefit from the new treatment under investigation compared to current treatments used in everyday practice. This study has also demonstrated the potential for running trials in a new way and so could have implications far beyond COPD.

Case Study courtesy of Understanding Patient Data

3.26 We agree with the NDG that the opt-out should not apply to anonymised information, in line with the ICO Code of Practice on Anonymisation.[15] The Information Governance Alliance (IGA) is developing new anonymisation guidance which will set out clear expectations for the health and social care system on how to meet the ICO Code of Practice on Anonymisation. The IGA will consult on this new guidance and publish it in 2018.

3.27 This is a complex area and we are aware that a number of organisations and health systems are looking at how best to anonymise data. We are keen to learn lessons from these to see how this could influence our approach to implementing the new national opt-out. This will build on existing best practice and take into account developments such as the UK data protection legislation.

Protecting anonymised information

3.28 In order for anonymised information to be shared, there needs to be robust assurance that this information is safe and secure and that the risk of re-identifying patients can be managed. Both the public and the professionals responding to the consultation made it clear that security is a key consideration.

> *"It is essential that the highest standards of security and safeguarding are in place to protect this information, and that the organisation responsible has the resources it needs to deliver this with confidence"*
>
> **Richmond Group of Charities**

3.29 The NDG recommended that the Government should consider introducing stronger sanctions to protect anonymised data, including criminal penalties for deliberate or reckless re-identification of individuals. This was overwhelmingly supported by respondents to the consultation. The implementation of stronger criminal sanctions would reassure those concerns.

> *"Stronger sanctions may help to increase service users' confidence on how their information is managed"*
>
> **Response from individual**

3.30 Many of the responses, especially from organisations representing patient groups, emphasised that, for these stronger sanctions to be applied appropriately and proportionately, they need to operate from clear definitions. In particular, they will need to distinguish clearly between deliberate, reckless and accidental re-identification of individuals.

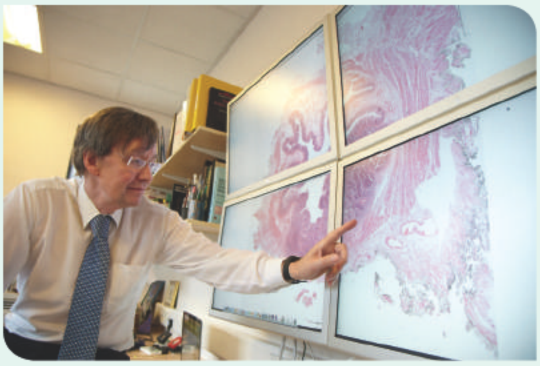
> *"Sanctions should be proportionate to the nature and scale of the breach"*
>
> **Wellcome Trust**

3.31 The Government is committed to implementing UK data protection legislation which, from May 2018, will provide a revised framework for protecting personal data and impose more severe penalties for data breaches and to deter reckless or deliberate misuse of information.

[15] Information Commissioner's Office, *Code of Practice on Anonymisation*, November 2012

Case Study: **Yorkshire Cancer Research**

Using health information to improve patient outcomes



Bowel cancer is the third most common type of cancer in England, with 4,668 cases diagnosed in Yorkshire in 2010. The rate of diagnosis has been rising across the Yorkshire and Humber region and deaths have been falling due to a better understanding of the disease through research.

To help improve bowel cancer care, researchers funded by Yorkshire Cancer Research are linking routine NHS datasets (such as HES, cancer registrations, screening, radiotherapy and chemotherapy), patient reported outcomes and diagnostic outcomes of bowel cancer patients across Yorkshire to assess the quality of hospital services and bowel cancer outcomes across the region.

This information will be used by a team of healthcare professionals caring for bowel cancer patients to identify where care can be improved and to start education initiatives to advance patient care. The programme aims to achieve a 10 15 per cent improvement in patient outcomes, preventing around 120 to 150 deaths from bowel cancer each year. National roll out could lead to even greater improvements in bowel cancer survival.

"Access to a wide range of health information and outcomes allows us to identify excellent and poor practice, design educational initiatives and improve overall care for bowel cancer patients. This saves lives and prevents unnecessary suffering." **Researcher perspective**

Case study courtesy of the Association of Medical Research Charities: 'a matter of life and death: how your health information can make a difference', 2016.

A continuing dialogue

3.32 During the consultation, a number of respondents raised several complex issues. Over the coming months there will be wide engagement with organisations, professionals and the public to ensure that a considered and well-rounded approach is taken to arrive at appropriate solutions.

3.33 From the charity sector, we had both queries and suggestions about how, or whether, the new national opt-out will interact with the national disease registries including those for cancer, congenital anomalies and rare diseases. The Government welcomes the work that Macmillan and Cancer Research UK have led on informing patients about their choices on the cancer registries. The Government agrees that Public Health England (PHE) should continue to strengthen existing opt-out arrangements for the cancer, congenital anomalies and rare diseases registries.

3.34 PHE will work with the cancer charities to take forward their recommendations. They will also work with people affected by cancer, congenital anomalies and rare diseases and with local care providers and national bodies, to ensure that patients have access to the information they need about the registries and that their requests to opt out will be respected. The cancer, congenital anomalies and rare diseases registries will, therefore, continue to operate separate opt-out mechanisms and will be exempt from the national opt-out when it is introduced. In time, there may be opportunities to integrate these registries with the new national opt-out. Once the national opt-out is in place, the potential impacts of any such future integration would be carefully explored with the cancer charities and the health and social care system.

3.35 The Government will continue to oversee work to ensure that nationally important data collections are held and managed in the best way to safeguard their value regarding improving the diagnosis and treatment of disease while, at the same time, respecting patient choices over who can access personal information about them.

3.36 To support this, PHE, the Department of Health and NHS Digital have asked Professor Keith McNeil, the Chief Clinical Information Officer for health and social care, to look at the role that NHS Digital could play in supporting the management of other national data collections, at the same time protecting the vital patient and population health and care services that these data collections support.

3.37 We also heard about the importance of patient surveys in understanding patient experience and acting as an early warning sign of poor quality and unsafe care. Organisations such as CQC and members of the research community raised concerns about the impact of an opt-out on the statistical validity of their surveys.

> *"Participation in the NHS Patient Survey Programme enables providers to compare their performance with others and therefore evidence the quality of their services"*
>
> **Care Quality Commission**

3.38 In response, the Department of Health will work with CQC, NHS England, NHS Digital, researchers and other interested bodies to assess any potential impact on statistical validity and quality and safety of care before reaching a full conclusion on this.

3.39 We are also keen to support the use of patient data in appropriate circumstances and anonymised data for research, and will learn from examples where this is being done effectively. The National Institute for Health Research Health Informatics Collaborative (NIHR HIC) is a collaboration between five leading NHS Trusts, each of which has a strong relationship with a partner university. The collaborative brings together clinical, scientific, and informatics expertise at each Trust and partner university to improve the quality and availability of patient information for research purposes and thereby improve patient outcomes and patient experience. One of the principal goals of the collaborative is to create a governance framework for data sharing and re-use across the Trusts and partner organisations, and to develop a data sharing agreement, allowing for the transfer of information between Trusts in a way which fully complies with relevant regulations.

Case Study: **Nicola's Story**

Public Health England's (PHE) National Disease Registration Service work on rapid diagnosis and avoidance of emergency presentations is at the centre of improving cancer survival.

Nicola Murrells was first diagnosed with cancer of the bowel in 2012, just after her little girl was born. As with over half of the rarer cancers like pancreatic and colon, her disease was diagnosed in her local A&E department in Manchester where she had gone after suffering excruciating stomach pains. She had surgery but, a year later, the cancer was back this time in her liver and colon. Nicola says she just could not face the chemotherapy she had had when she was first diagnosed and wanted to live as normal a life as possible with her daughter and husband Steve.

But, Nicola is a fighter too. And while she did have further surgery, the spread of the disease meant that removing the tumours completely just was not possible. A year ago she was told she would probably not live longer than six to nine months. She opted to go on one of the many trials of new immunotherapy drugs that are at last providing some hope in the battle against this terrible disease.

This is where the work of the National Cancer Registration and Analysis Service is providing a possible lifeline to people like Nicola. It collects data on all cancer treatments, however the patient enters the NHS cancer care system and shows which drugs and treatments are working and just as important, which ones are not. Sharing information safely and securely online making sure that a specialist treating a patient in Peterborough can see in an instant what is working for a similar patient in Penzance is vital when it comes to finding a cure.

Nicola is still alive today. Her tumours have not shrunk, but they are not growing either. Something seems to be working although her doctors do not yet know why. In fact, Nicola is more than alive she is living life to the full, raising money for cancer charities, enjoying holidays with her husband and of course, looking after her younger daughter.

Case Study courtesy of Public Health England

Supporting professionals

3.40 There was a broad consensus that the implementation of any new model, process or system would need to be accompanied by clear, timely and consistent communications and guidance to support those professionals and practitioners who will be key for smooth roll-out. We heard this particularly strongly from organisations that represent health and care professionals and local authorities, who will all be at the forefront of any implemented change. The suggestions for the type of support that will be needed ranged from clarity of terminology and purpose, clear and timely communications and guidance, through to practical resources and an effective, workable technical solution.

"This should fully embrace the role that health and care staff need to play in communicating to patients the issues and practicalities that underpin the use and management of personal health data, and this should include those staff that support patient groups, or undertake patient participation work"

Royal College of Nursing

3.41 We will engage with relevant organisations and users to ensure that the tools and support for frontline staff are informed by the needs of those concerned. This will draw on best practice from across the health and social care system.

"Communication, Communication, Communication"

3.42 In her review, the NDG made it clear that it is not enough just to make people's choices simpler, but that their choice also needs to be informed. We recognise that there is a need to communicate clearly not only about the right to opt out but also about how data is used, the benefits it can bring to research and to improving the NHS and social care system, and how it is protected and safeguarded. The consultation responses from organisations, professionals and the public across the board firmly reflected this assertion.

3.43 In addition to extensive engagement with a range of stakeholder groups, we have established a Programme Advisory Group, drawn from health and social care and the third sector, to enable us to listen, learn and take expert advice from those who are closest to professionals, patients and the public as we work to implement the new national opt-out. Our communications and engagement approach will reflect what professionals, patients and the public have told us they need to know and understand in order to make an informed choice and be confident in the health and social care system's ability to use and safeguard their data responsibly and securely. We will ensure our wider communications are grounded in the tangible benefits of making data available, both on an individual basis and in the context of the wider health and social care system, and that the opt-out process is easy to understand and to engage with.

"DH and the NDG will need to lead a national information campaign to ensure that patients are provided with clear information… to help them make an informed choice about whether or not to opt out"

Public Health England

3.44 Data and security issues, the choices that people can make, and how data is accessed and used, can often seem confusing and complicated, surrounded by jargon and technical language. We recognise the reflections of both the NDG, and also of many of the professional organisations that responded to the consultation, that the opt-out, the way we present it and the benefits from using data, need to be greatly simplified if we are to increase public understanding and, in turn, earn their trust and confidence.

"A significant number of the public are not sure who will have access to data about them or what it will be used for"

Royal College of General Practitioners

Case Study: **Barbara's Story**

PHE's National Disease Registration Service is working with rare cancer charities to provide the data that is transforming the lives of patients.

Three years ago, when Barbara was 76, she went to see her GP. She had had a nasty cough for over a month; sometimes she coughed up blood and was losing weight. She knew it could be bad news and was frightened. Barbara was sent for urgent x rays and scans. The results were not good   the lymph glands in her chest were enlarged and there were some quite large suspicious lumps in her liver.

A former lawyer and civil servant, Barbara knew that the data about lung cancer showed that her life with a diagnosis of advanced lung cancer was going to be short. She and her family contacted Marie Curie, the charity that supports people living with terminal illness, and began to discuss the palliative care options for her remaining months.

Her oncologist, however, did not feel the picture was quite right and persuaded her family that it was worth a biopsy of the lumps and masses in Barbara's liver   just to make sure. Barbara was less keen, but agreed and the tests went ahead. The oncologist's hunch was correct   they were not related to the supposed lung cancer but a very rare, slow growing neuroendocrine tumour which was treatable, because her doctors had managed to catch it soon enough. Her cough, it turned out, was from an infection on a pre existing lung disease and responded well to antibiotics.

It was the data that then guided her treatment. Neuroendocrine cancers, which attack the hormone and nervous systems, are rare, so it is difficult to know how best to treat them. But the data on England's National Cancer Registration and Analysis Service is some of the best in the world   and the team in PHE work with the neuroendocrine cancer charities and patient groups. This work is beginning to show us that with new treatments such as radiolabelled antibodies, which deliver radioactive treatment directly to the cancer cells, these cancers can often be controlled.

The tumour shrank dramatically with the intervention and Barbara has gone on to live another three years   and, most importantly for her, to see her first grandchild born.

Case Study courtesy of Public Health England

> *"Options to opt out must be made widely known to the public. Many people I speak to have no idea that there is a discussion concerning their medical data. There would need to be a hugely significant, honest and clear public information campaign"*
>
> **Response from individual**

3.45 We greatly value the work of the Wellcome Trust and its 'Understanding Patient Data' initiative. This is developing a common and accessible language to build greater understanding of what patient data is and how it can be used to benefit individual patients and the health and social care system more widely, such as through supporting the running of the NHS and enabling research. This work is helpful and will inform the way in which people make effective and fully-informed decisions.

Taking the time to get it right

3.46 The NDG stressed the importance of taking the time to ensure that the implementation of the new data security standards and the national opt-out would not cause disruption or confusion for professionals and the public. This message was reinforced through the consultation.

> *"Take sufficient time to get this model right: there is a great deal of careful work that needs to be done"*
>
> **Wellcome Trust**

3.47 In order to move from 'principle' to 'practice', our next steps will be characterised by careful planning for implementation and an orderly transition from the current system. This is set out in the implementation plan at Annex G. During this time there will be a national dialogue and engagement with professionals and the public to ensure that decisions and changes reflect the recommendations of the NDG, the needs of the health and social care system, and what we heard during the consultation.

4. Equality Issues

Case Study: **Southall and Brent Revisited (SABRE)**

Investigating trends in diabetes

Diabetes is a pressing health issue for the UK. It is critical to learn more about the causes of diabetes to understand how to prevent it. Healthcare professionals and researchers want to understand why diabetes seems to affect different groups of people in different ways.

SABRE is a large scale study, funded by the British Heart Foundation and Wellcome, and run by a team based at University College London with support from the Universities of Bristol, Cambridge, Edinburgh, Exeter, Glasgow, Newcastle, Oxford and Washington (Seattle, USA).

In 1988, 5,000 people of European, South Asian and African Caribbean origin living in North West London were recruited onto the SABRE study. This work looks at the causes of diabetes and cardiovascular disease, and why some people stay well in older age while other people experience illness and disability. Participants were followed up between 2008 and 2011, and are now being invited to a 25 year follow up. Researchers collected information on those studied, including health and lifestyle surveys, blood pressure measurements, GP and hospital health records.

The SABRE study has contributed significantly to our understanding of how ethnicity can affect the risk of developing diabetes. It has shown that 50 per cent of people with South Asian, African and African Caribbean origins will develop diabetes by the time they are 80. This kind of information is invaluable in targeting specific groups with prevention messages and early diagnosis initiatives.

Data was collected from GP and hospital records, as well as directly from the study participants. Participants gave their consent for data to be collected from GP records (this was anonymised according to the ICO Code of Practice and was not linked to identifiable information) and for the data that they had given directly to be used in the research. Data from hospital records was provided by the NHS Health and Social Care Information Centre (now NHS Digital), under a Section 251 approval. Hospital record linkage is conducted within NHS Digital.

Case study courtesy of Understanding Patient Data

4.1 Reinforcing the need for good communication and further engagement, many of the responses we received raised the need for us to pay particular attention to ensuring that communications and messaging are widely accessible, reflecting unique needs, to ensure that no one would be left out of the conversation.

> *"Further consideration should be given regarding those people who require additional support (e.g. reliance on self-serve websites is not appropriate for all service users)"*
>
> **Local Government Association**

> *"The implementation and communication of them must be undertaken in line with the Accessible Information obligations and to ensure clarity of message to all groups"*
>
> **Response from individual**

4.2 We agree that everyone needs to be able to make a meaningful and informed choice about how their information is used, and also to be able to understand how their information is protected. The voluntary sector will be involved in taking forward plans to define, communicate, and implement the new approach to opt-outs to understand fully the needs of all and ensure that communications work for all groups. This will include providing accessible information, advice and tools to professionals to enable them to support people in making their own decisions, or to support professionals and carers to reach a decision where someone does not have capacity to do so themselves. This will also inform the design of the national opt-out, so that both the question and the methods available for opting out will be easy to use.

4.3 We also heard concerns from respondents, especially from the charity and research communities and regulatory bodies, about the potentially disproportionate impact that opt-outs could have on both medical research and the uses of data for service monitoring and improvement, as this could bias the end results.

> *"As currently worded, the opt-out would affect both national and local survey activity run either by trusts or national bodies such as CQC or NHS England"*
>
> **Care Quality Commission**

> *"The specificity and sensitivity of the analyses...depends on the completeness of the data upon which these analyses are based"*
>
> **Public Health England**

4.4 We agree with the charity and research communities and regulatory bodies that sharing information carefully and sensitively offers immense potential, for improving health and care services and outcomes. There is great potential for example, in using research to redress health inequalities, especially in terms of how we design and improve our services so that they meet the needs of vulnerable groups. We acknowledge the importance of sharing information appropriately for important purposes, such as the safeguarding of vulnerable children and adults.

4.5 We recognise that there are different needs across the country and there are examples of local areas sharing data in safe and secure ways to better understand and respond to patients' needs and improve services. These include the Leeds Care Record which covers data from GP practices, hospitals and mental health, with community services and social care to be added; and the Whole System Integrated Care record (WSIC) enabling information sharing between health and social care in North West London. These highlight the potential for more local areas sharing data to improve care, outcomes, support and services.

4.6 We remain committed to using every opportunity for reducing health inequalities, and we recognise that enabling the flow of data for research and system improvement can be a hugely beneficial way of achieving this, to explore both the causes of health inequalities and the solutions. In designing and implementing the new national opt-out we will ensure this benefit can continue to be realised and will also keep the impacts on people with different equality protected characteristics under review.

5. Patient Empowerment

5.1 Better use of data and technology has the power to improve health and clinical outcomes, deliver better patient experience, transform the quality of care to the individual, improve the NHS and support a more efficient health and social care system. The NDG review is one important part of achieving that.

5.2 At the heart of this is the opportunity to put individuals in the driving seat in the management and control of their own health and care. We are creating new digital health tools (online, mobile and apps) that will give all of us the information we need to make good decisions and informed choices about the health and care provision most appropriate to our individual needs. They will make health and care more accessible, more convenient and more effective for everyone.

5.3 Data and technology will enable a better experience for staff by reducing bureaucracy and making the most of the unique opportunities that technology can offer to support clinicians to provide more personalised and responsive advice, care and treatment. Using information and technology will mean more of the patient conversation with the clinician will focus on their immediate care needs, rather than repeating the often unnecessary and distracting case history of past care.

5.4 NHS.UK is being created to replace NHS Choices and is due to be launched in September 2017. It will connect individuals to a vast range of health and care information and the services they need to help them to manage their health and wellbeing. Patients will be able to access personalised content, specific to their needs, helping to make better, informed choices and guiding people to the care that they need faster and more directly.

5.5 We will offer everyone the opportunity to book appointments online, with a clinician and carer of their choice, at a time and place that suits them best.

5.6 Technology will support more accurate diagnosis by eliminating errors caused by incomplete or inaccurate notes and records. It will remind patients to order repeat prescriptions online when they need them and have them dispensed at a place and time that meets the needs of their lives. We want patients to have the choice to receive online consultations if that is what they want and if it is appropriate.

5.7 We will create NHS111 online as part of the existing 111 service, integrating it with NHS.UK. This will enable patients to be triaged online for a limited number of low risk conditions, providing real-time access to information to clinicians in A&E, 111 and 999 to inform and speed up diagnosis.

Case Study: **Diabetes UK**

Putting Feet First

20 people a day have a foot, leg or toe amputated as a result of diabetes, but 4 out of 5 of these amputations are preventable. These unnecessary amputations cause suffering to the people involved and are a waste of NHS resources.

Diabetes UK is a partner to the National Diabetes Audit, which links Hospital Episode Statistics (HES) to primary care data to identify areas of the country where the problem of preventable amputation is particularly severe in order to work with those areas to improve awareness and ensure more targeted treatment to reduce unnecessary amputations. This analysis, demonstrating the extent and regional variation of the problem, provided the evidence that has been put to use by developing Putting Feet First.

Putting Feet First is a UK campaign, run by Diabetes UK, to reduce the number of preventable amputations linked to diabetes. This campaign includes encouraging people with diabetes to be more aware of the possible symptoms that can lead to the need for amputation and what to do if they notice these symptoms. This can support healthcare professionals to take the right approach to diabetic foot care, and encourage commissioners and NHS planners to deliver an integrated foot care pathway that ensures people with diabetes get the right treatment at the right time.

By pinpointing exactly where in the UK this problem is particularly severe, Diabetes UK is able to target its resources and support commissioners and planners where improvement is most urgently needed.

Case study courtesy of Understanding Patient Data

5.8 During this year we will launch a series of apps relating to prevention and mental health as part of the NHS ‘digital tool’ library on NHS.UK. Self-care apps will provide the patient and clinician with valuable data on patients’ health, enabling clinicians to monitor patients’ health remotely and so reduce the burden on the frontline.

5.9 Patients can already access their summary care record. In future they will be able to add their own comments and link their record to technological innovations such as wearable devices that will help them monitor their own health.

5.10 The NDG recognised that data security and the trust of patients in how their data is used are vital, if we are to achieve the technological advances that will empower patients to take control of and manage their health and care. This Government response has set out what we will put in place to protect people’s data, to ensure that it is held safely and securely and to help people understand the choice they have about how it is used.

Annex A: Response to the National Data Guardian's Recommendations

The Government agrees with all of the recommendations made by the NDG. Further details on our response to each of the recommendations are provided below.

Recommendation	Government Response
Data Security	
1 The leadership of every organisation should demonstrate clear ownership and responsibility for data security, just as it does for clinical and financial management and accountability.	**Agree**. The Government supports increased ownership of data security among health and care leaders (including Boards) who will be a key audience of the communications campaign. Ensuring that local Boards are implementing the 10 data security standards will be a factor considered by CQC and NHS Improvement in decisions to apply their regulatory powers. In summer 2017, NHS Improvement will publish a new 'statement of requirements' which will clarify required action for local organisations in 2017/18. Chief Executive Officers must respond to this with an annual 'statement of resilience', confirming essential action to ensure that standards are being implemented. This will include the requirement for each organisation to have a named executive Board member responsible for data and cyber security.

Recommendation	Government Response
2 A redesigned Information Governance Toolkit should embed the new standards, identify exemplar organisations to enable peer support and cascade lessons learned. Leaders should use the Information Governance Toolkit to engage staff and build professional capability, with support from national workforce organisations and professional bodies.	**Agree.** NHS Digital will implement a redesigned Information Governance Toolkit to support the new standards, testing in 2017 and going live in April 2018.
3 Trusts and CCGs should use an appropriate tool to identify vulnerabilities such as dormant accounts, default passwords and multiple logins from the same account. These tools could also be also used by the IT companies that provide IT systems to GPs and social care providers.	**Agree.** The redesigned Information Governance Toolkit will signpost Trusts, CCGs, GP systems suppliers and social care providers, to appropriate tools to identify such vulnerabilities.
4 All health and social care organisations should provide evidence that they are taking action to improve cyber security, for example through the 'Cyber Essentials' scheme. The 'Cyber Essentials' scheme should be tested in a wider number of GP practices, Trusts and social care settings.	**Agree.** All health and care organisations will need to provide evidence of their efforts to improve cyber security through the redesigned Information Governance Toolkit, being tested in alpha and beta versions in 2017, prior to being introduced by April 2018. This will be used by organisations themselves and by regulators to assure that data security standards are implemented. We will work with a range of health and care organisations through the redesigned Information Governance Toolkit to assess whether 'Cyber Essentials Plus' meets their needs. We will ensure that the redesigned Toolkit, will signpost organisations towards the appropriate assurance framework for them.

Recommendation		Government Response
5	NHS England should change its standard financial contracts to require organisations to take account of the data security standards. Local government should also include this requirement in contracts with the independent and voluntary sectors. Where a provider does not meet the standards over a reasonable period of time, a contract should not be extended.	**Agree.** We will work with NHS England and through local authorities in England, the LGA and ADASS, to embed the data security standards in contracts where appropriate. The standards are already reflected as requirements in the NHS Standard Contract and GMS Contract for 2017/18 which came into force in April 2017.
6	Arrangements for internal data security audit and external validation should be reviewed and strengthened to a level similar to those assuring financial integrity and accountability.	**Agree.** The redesign of the Information Governance Toolkit will provide a platform for strengthened assurance around data security. It is being tested in alpha and beta versions in 2017, prior to being introduced by April 2018.
7	CQC should amend its inspection framework and inspection approach for providers of registered health and care services to include assurance that appropriate internal and external validation against the new data security standards have been carried out, and make sure that inspectors involved are appropriately trained. HSCIC should use the redesigned Information Governance Toolkit to inform CQC of 'at risk' organisations, and CQC should use this information to prioritise action.	**Agree.** Data security will form part of CQC's well-led inspection framework from September 2017, which will be supported by information from the redesigned Information Governance Toolkit from April 2018.

	Recommendation	Government Response
8	HSCIC should work with the primary care community to ensure that the redesigned Information Governance Toolkit provides sufficient support to help them to work towards the standards. HSCIC should use the new toolkit to identify organisations for additional support, and to enable peer support. HSCIC should work with regulators to ensure that there is coherent oversight of data security across the health and social care system.	**Agree.** NHS Digital will work with the primary care community in developing the redesigned Information Governance Toolkit being tested in alpha and beta versions in 2017, prior to being introduced by April 2018. The new service will take into account the relative needs and expectations of organisations of different sizes when considering their data security capability. We expect the redesigned Information Governance Toolkit to facilitate the identification of those organisations in need of additional support.
9	Where malicious or intentional data security breaches occur, the Department of Health should put harsher sanctions in place and ensure the actions to redress breaches proposed in the 2013 review are implemented effectively.	**Agree.** The new 2018 UK data protection legislation will provide a framework for protecting personal data and will impose more severe penalties to deter intentional or reckless misuse of information.

Data Sharing and Opt-Out

10	The case for data sharing still needs to be made to the public, and all health, social care, research and public organisations should share responsibility for making that case.	**Agree.** The Government will work with health, social care, research and public organisations to ensure that the benefits of data sharing are included in future public communications.
11	There should be a new consent/opt-out model to allow people to opt out of their personal confidential data being used for purposes beyond their direct care. This would apply unless there is a mandatory legal requirement or an overriding public interest.	**Agree.** The Government agrees with the need to simplify the means by which people can opt out and will engage fully towards implementing this.
12	HSCIC should take advantage of changing its name to NHS Digital to emphasise to the public that it is part of the NHS 'family', while continuing to serve the social care and health system as a whole.	**Agree.** The Health and Social Care Information Centre (HSCIC) was renamed NHS Digital on 1 August 2016 and is already realising the benefits from this change.

Recommendation	Government Response
13 The Government should consider introducing stronger sanctions to protect anonymised data. This should include criminal penalties for deliberate and negligent re-identification of individuals.	**Agree.** We are putting stronger sanctions in place by May 2018, through UK data protection legislation, to protect against anonymised information being re-identified through recklessness or deliberate intent.
14 The forthcoming IGA's guidance on disseminating health and social care data should explicitly refer to the potential legal, financial, and reputational consequences of organisations failing to have regard to the ICO's Code of Practice on Anonymisation by re-identifying individuals.	**Agree.** The Information Governance Alliance (IGA) will publish anonymisation guidance drawing on the ICO's Code of Practice on Anonymisation in 2018.
15 People should continue to be able to give their explicit consent, for example to be involved in research.	**Agree.** We will continue to uphold this principle.
16 The Department of Health should look at clarifying the legal framework so that health and social care organisations can access the information they need to validate invoices, only using personal confidential data when that is essential.	**Agree.** The Government will look for an early opportunity to clarify the legal framework by working with the Confidentiality Advisory Group (CAG) to ensure its approvals process under Section 251 of the NHS Act 2006 enables organisations to access the data they need.
17 The Health Research Authority should provide the public with an easily digestible explanation of the projects that use personal confidential data and have been approved following advice from the Confidentiality Advisory Group.	**Agree.** The Health Research Authority acknowledges this recommendation and is considering further steps, including a technological solution to make its register more accessible.

Recommendation

18 The HSCIC should develop a tool to help people understand how sharing their data has benefited other people. This tool should show when personal confidential data collected by HSCIC has been used and for what purposes.

Government Response

Agree. NHS Digital will update its data dissemination register to be more explicit about the purposes that the data they disclose has been used for, and will include the benefit described by the data applicant in their application. By December 2018, people will be able to access a digital service to help them understand who has accessed their summary care record. By March 2020, it will also enable people to use online services to see how their data collected by NHS Digital has been used for purposes other than their direct care.

Next Steps

19 The Department of Health should conduct a full and comprehensive formal public consultation on the proposed standards and opt-out model. Alongside this consultation, the opt-out questions should be fully tested with the public and professionals.

Agree. We have consulted and this document sets out our response to the public consultation. We will continue to engage with the public and professionals.

20 There should be ongoing work under the National Information Board looking at the outcomes proposed by this consultation, and how to build greater public trust in data sharing for health and social care.

Agree. The National Information Board will continue to consider how to build greater public trust in data sharing for health and social care.

Annex B: Response to the Care Quality Commission's Recommendations

The Secretary of State for Health asked the Care Quality Commission (CQC) to review the effectiveness of current approaches to data security by NHS organisations when it comes to handling patient data, and make recommendations on how current arrangements for ensuring NHS providers protect data could be improved. He also asked CQC to make recommendations about how the new guidelines (published by the NDG, Dame Fiona Caldicott) can be assured through CQC inspections, NHS England commissioning processes, and any other potential mechanisms. CQC's 'Safe Data, Safe Care' review was published in July 2016.

Recommendation	Government Response
1 The leadership of every organisation should demonstrate clear ownership and responsibility for data security, just as it does for clinical and financial management and accountability.	**Agree.** The communication campaign will target leaders as a key group to support them in taking greater ownership.
2 All staff should be provided with the right information, tools, training and support to allow them to do their jobs effectively while still being able to meet their responsibilities for handling and sharing data safely.	**Agree.** Both the communications campaign and the data security training will support staff in meeting their responsibilities.
3 IT systems and all data security protocols should be designed around the needs of patient care and frontline staff to remove the need for workarounds, which in turn introduce risks into the system.	**Agree.** This recommendation will be overseen by the National Information Board to ensure new systems reduce security risks while remaining user friendly.
4 Computer hardware and software that can no longer be supported should be replaced as a matter of urgency.	**Agree.** Organisations will be expected to update systems and to manage risks where that is not immediately possible. Guidance on removing unsupported software will be issued in July 2017. In autumn 2017, the Chief Information Officer for health and social care will set out further action needed to address technology which risks safe patient care. A framework will be in place to support organisations to move to the latest operating system by March 2018.

Recommendation	Government Response
5 Arrangements for internal data security audit and external validation should be reviewed and strengthened to a level similar to those assuring financial integrity and accountability.	**Agree.** The new assurance framework will put data security onto a similar footing to financial integrity and accountability.
6 CQC will amend its assessment 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 involved are appropriately trained.	**Agree.** The Government welcomes the inclusion of data security in the CQC's well-led inspection framework.

Annex C: Consultation questions

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 for an event to be held?

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?

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?

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[16], or NHS England would you find helpful in implementing the ten standards?

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

Question 11: Do you have any comments or points of clarification about any of the eight elements of the model?

[16] The Health and Social Care Information Centre was renamed NHS Digital on 1 August 2016 in line with the National Data Guardian's recommendation 12.

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?

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

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?

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?

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?

Annex D: The National Data Guardian's 10 Data Security Standards

Leadership Obligation 1

People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

Data Security Standard 1: All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful and appropriate purposes.

Data Security Standard 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.

Data Security Standard 3: All staff complete appropriate annual data security training and pass a mandatory test, provided through the redesigned Information Governance Toolkit.

Leadership Obligation 2

Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

Data Security Standard 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 instances of access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5: Processes are reviewed at least annually to identify and improve any which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Data Security Standard 6: Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken as soon as possible following a data breach or near miss, with a report made to senior management within 12 hours of detection. Significant cyber-attacks are to be reported to CareCERT immediately following detection.[17]

[17] Original wording of Data Security Standard 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

Data Security Standard 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.

Leadership Obligation 3

Technology: Ensure technology is secure and up-to-date.

Data Security Standard 8: No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9: A strategy is in place for protecting IT systems from cyber threats, based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10: IT suppliers are held accountable via contracts for protecting the personal confidential data they process and for meeting the National Data Guardian's data security standards.

Annex E: The National Data Guardian’s 8 Point Model

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 healthcare 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:

- **A.** Personal confidential information being used to provide local services and run the NHS and social care system.
- **B.** Personal confidential information being used to support research and improve treatment and care.

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 (ICO) 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 of Practice.

The Health and Social Care Information Centre,[18] 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. Arrangements will continue to cover exceptional circumstances.

The opt-out will not apply where there is a mandatory legal requirement or an overriding public interest.

These will be areas where there is a legal duty to share information (for example a fraud investigation) or an overriding public interest (for example to tackle the ebola virus).

[18] The Health and Social Care Information Centre was renamed NHS Digital on 1 August 2016 in line with the National Data Guardian's recommendation 12.

Annex F: Consultation Analysis and Summary of Responses

1. Executive Summary

Background:

- The Department of Heath consulted with health and care professionals and organisations and the public to seek their views on the proposed data security standards and the new national opt-out. This has informed the Government's response to those recommendations.
- The consultation combined formal written consultation methods with interactive events in order to gain valuable and substantive feedback from a wide range of stakeholders including practitioners, local leaders and the public.

Headline Findings:

- There is broad support for having a robust framework of data security standards, as proposed by the National Data Guardian (NDG).
- There is broad support for having a national opt-out, as proposed by the NDG.
- Trust is key and needs to be earned by making the case for the benefits of sharing data in a safe, secure and meaningful way.
- There needs to be an improved understanding about how information moves around the health and social care system, and why it needs to do so, for the public to make an informed choice.
- The new data security standards, along with clear information about security and accountability, will help to provide reassurance and build trust.
- There is a need for very clear and well-articulated terminology to avoid confusion or a lack of consistency.
- Good communications, guidance and accessible sources of advice will be needed to ensure that the public are aware of, and engaged in, the changes and can make an informed choice about whether or not to opt out.

- Good communications, guidance, support and lead-in time will be needed to support practitioners and local leaders to implement the new data security standards and the new national opt-out effectively.
- It is essential that communications are ongoing, consistent, coordinated and targeted.
- Delivery plans need to take into account the resource pressures (time, money and people) surrounding the delivery of any new data security standards or new national opt-out.
- There are concerns about the challenge of implementing both the data security standards and the national opt-out across a complex context of different organisations and settings.

2. The Consultation Process

- The consultation on '*New Data Security Standards and Opt-Out Models for Health and Social Care*' took place over a 2 month period, beginning on 6 July 2016 and ending on 7 September 2016.
- The consultation sought views on the NDG's recommendations, including:
  - 10 new data security standards
  - A new 8 point model for data sharing in health and social care
- The consultation document and feedback form was made available on the gov.uk website at **https://consultations.dh.gov.uk/information/ndg-review-of-data-security-consent-and-opt-outs** and a dedicated inbox was set up to receive feedback directly.
- Three 'listening' events were held to meet with a wide range of stakeholders and explore the review in more depth. Each event included a session for professionals and a session for members of the public.
- The events took place in London (26 September 2016), Southampton (3 October 2016), and Leeds (10 October 2016), and were attended by 111 practitioners and 67 members of the public in total.
- The majority of practitioners came from information governance, IT or other corporate services. Those more directly involved in providing healthcare were less well represented. Members of the public generally held a role as a patient or service user representative.

3. Details of consultation responses received

- There were 638 responses to the consultation. 552 were submitted through the online consultation hub and 86 were submitted directly to the consultation inbox. The breakdown of responses by type is shown below.

Online Respondents:

Member of the Public	381 (69.02%)
Hospital Trust or Foundation Trust	20 (3.62%)
Arm’s Length Body	7 (1.27%)
Social Care Provider	4 (0.72%)
Government Department	2 (0.36%)
Commissioning Support Unit	3 (0.54%)
General Practitioner	13 (2.36%)

Local Authority	10 (1.81%)
Professional Organisation/ Association	12 (2.17%)
Research Body	9 (1.63%)
Clinical Commissioning Group	9 (1.63%)
Public Health Organisation	1 (0.18%)
Special Interest Group	8 (1.45%)
Other	37 (6.70%)

Responding in a personal or private capacity:

Personal: 63 (11.41%)	Private: 121 (21.92%)	Not Answered: 368 (66.67%)

The Questions that attracted the most attention (over 50% response rate) were:

Question 4: **293 (53.1%)**
(Providing views on the 10 data security standards)

Question 12: **408 (73.9%)**
(Identifying levels of support for the proposals of stronger sanctions)

Question 15: **477 (86.4%)**
(Views on what needs to be done to move from the current opt-out model to the new one)

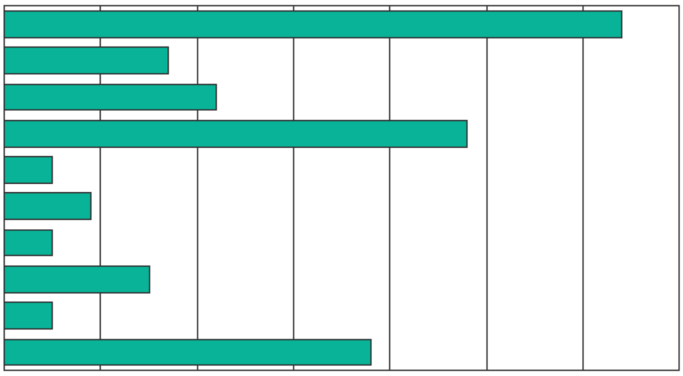
Question 4

The review proposes ten data security standards relating to leadership, people, processes and technology. Please provide your views about these standards.

Response rate: 293 (53.1%)

Specific data security standards commented on:

64	(11.59%)	Standard 1
17	(3.08%)	Standard 2
22	(3.99%)	Standard 3
48	(8.7%)	Standard 4
5	(0.91%)	Standard 5
9	(1.63%)	Standard 6
5	(0.91%)	Standard 7
15	(2.72%)	Standard 8
5	(0.91%)	Standard 9
38	(6.88%)	Standard 10



Question 5

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

Response rate: 155 (28%)

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?

Response rate: 199 (36%)

Question 7

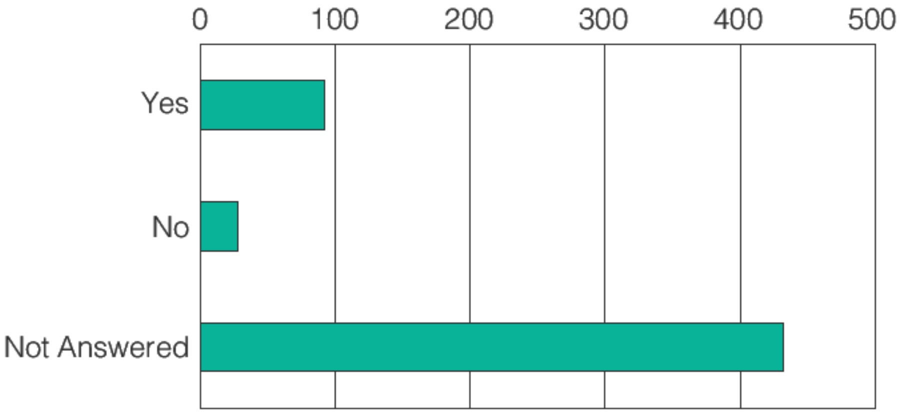
Please describe any particular challenges that organisations which provide social care or other services might face in implementing the ten standards.

Response rate: 176 (32%)

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

Response rate: 170 (31%)



Yes: 92 (17%) No: 28 (5%) Not Answered: 432 (78%)

Question 9

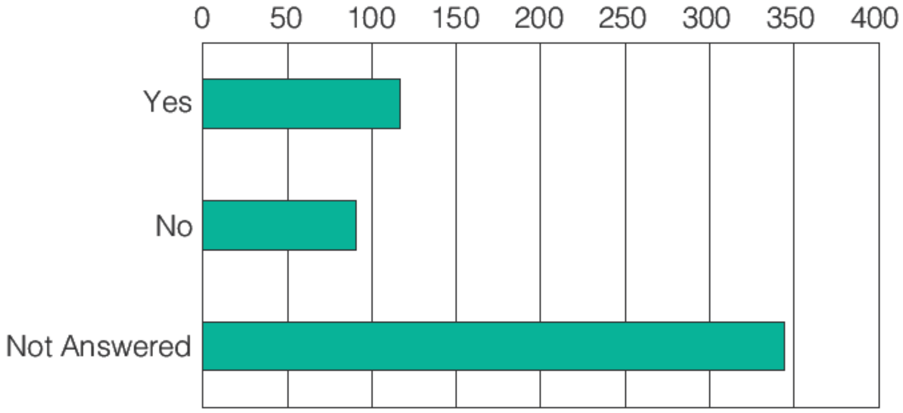
What support from the Department of Health, the Health & Social Care Information Centre, or NHS England would you find helpful in implementing the ten standards?

Response rate: 161 (29%)

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?

Response rate: 237 (43%)



Yes: 117 (21%) **No:** 91 (17%) **Not Answered:** 344 (62%)

Question 11

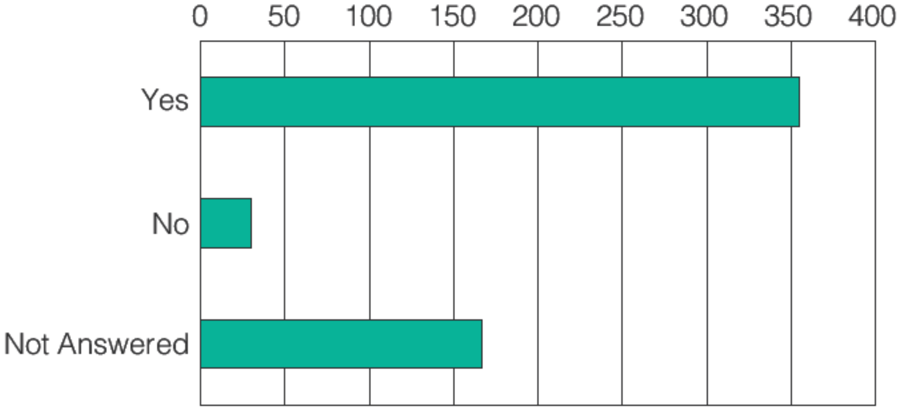
Do you have any comments or points of clarification about any of the eight elements of the model described above?

Response rate: 295 (53%)

Question 12

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

Response rate: 408 (74%)



Yes: 355 (64%) **No:** 30 (6%) **Not Answered:** 167 (30%)

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?

Response rate: 127 (23%)

Question 14

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

Response rate: 263 (48%)

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?

Response rate: 477 (86%)

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?

Response rate: 207 (38%)

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.

Response rate: 177 (32%)

Annex G: Implementation Plan

1. In 2015, the Secretary of State for Health commissioned the National Data Guardian for Health and Care (NDG) and the Care Quality Commission (CQC) to undertake reviews on data security and data sharing in the health and social care system. Those reviews were published in July 2016, and were followed by a public consultation, between July and September 2016, on the NDG's proposed data security standards and national opt-out.

2. The Government accepts the recommendations of the NDG and CQC reviews, including the 10 data security standards recommended by Dame Fiona, and her proposed national opt-out.

3. This high level implementation plan sets out the timescales for how we plan to deliver key actions on cyber security and data sharing.

Cyber resilience for the health and social care system

4. For the health and social care system, a significant programme of work is already underway to mitigate data and cyber security risks. In 2015, the Government created CareCERT, part of the newly created Data Security Centre in NHS Digital, to support health and care organisations to be more cyber resilient and respond to incidents promptly when they happen, working with the National Cyber Security Centre (NCSC). Over £50 million will be made available from 2015 to 2020 to support the CareCERT suite of services.

5. The cyber incident in May 2017 was the largest ransomware incident observed to date, affecting services in many other countries, as well as the NHS in the United Kingdom. This attack reaffirmed the potential for cyber incidents to impact directly on frontline care. Following this incident, Will Smart, the Chief Information Officer (CIO) of the health and social care system has begun a lessons-learned review, to report in October 2017 and inform further action.

6. Immediate lessons have already been identified from the incident, including:

- The need to ensure organisations implement critical CareCERT alerts, including software patches, and keep anti-virus software up to date. NHS England and NHS Improvement are already following up the small number of critical CareCERT alerts within 48 hours to confirm that local organisations have taken necessary action – starting now with major trauma units and Ambulance Trusts, and rolling out more widely in summer 2017.
- The need for organisations to identify and prioritise action to move away from or isolate unsupported systems; local organisations should be aiming to have isolated, moved away from, or be actively managing any unsupported systems by April 2018.
- Ensuring that organisations, their Boards and their staff, are taking the cyber threat seriously, understand the direct risks to frontline services and are working pro-actively to maximise their resilience and minimise impacts on patient care.

The plan set out below, centres on ensuring local organisations are implementing the 10 data security standards supported by the CareCERT suite of national support services, and backed up by clear contractual obligations and by assurance and regulatory action.

7. Boosting cyber resilience and improving the response to cyber incidents remains an urgent priority. Our priorities for action are:

- Establishing a clear contractual and regulatory framework.
- Addressing infrastructure weaknesses.
- Communications, engagement and training, to staff and leaders in the system.
- Building local performance and boosting capability.
- Improving threat surveillance and incident response.

8. **On the contractual and regulatory framework:**

- **NHS England** has ensured that the 10 data security standards are reflected as requirements for the NHS Standard Contract and General Medical Services (GMS) Contract requirement, which came into force in April 2017.
- **CQC and NHS Improvement** are responsible for maximising the use of their roles as regulators to ensure that Boards are implementing the 10 data security standards, and that this is considered in decisions to apply regulatory powers. In June 2017, CQC published its inspection framework for NHS Trusts, including data security as part of well-led inspections, and the first inspections of Trusts will begin in September 2017.
- **CQC** is consulting on new inspection frameworks for GPs and adult social care and these are planned to be published later in 2017.
- **NHS Improvement** will publish a ‘statement of requirements’ in summer 2017 to underpin the data security standards and the NHS Standard Contract requirements, to clarify required action for local organisations, and also ensure that Chief Executive Officers confirm in an annual ‘statement of resilience’ the actions they are taking to meet those requirements. This will include the requirement for each organisation to have a named executive Board member responsible for data and cyber security.
- **The Department of Health and NHS Digital** have already begun developing and testing proposed metrics, under the work to redesign the Information Governance Toolkit to go live in April 2018.
- **The Network and Information Security (NIS) Directive**, to be implemented by May 2018, will give further legal backing to the 10 data security standards by requiring those organisations identified as ‘operators of essential services’ to comply with defined security requirements.

9. Specific action has been taken since the May 2017 ransomware incident to ensure that organisations are required to implement cyber security CareCERT alerts. NHS England and NHS Improvement wrote to every NHS Trust, Clinical Commissioning Group (CCG) and Commissioning Support Unit (CSU) in May asking Boards to confirm that they have implemented all of the 39 CareCERT alerts issued by NHS Digital in the previous 3 months and taken essential action to secure local firewalls. NHS England and NHS Improvement have contacted every major trauma centre and Ambulance Trust. NHS Digital created a new CareCERT Collect system in June, providing assurance that

cyber alerts have been implemented. NHS England and NHS Improvement will follow up critical CareCERT alerts reported through the CareCERT Collect system within 48 hours to confirm that local organisations have the necessary plans in place.

10. **To address infrastructure weaknesses,** the Government is making £21 million of capital funding available in 2017/18 to increase the cyber resilience of major trauma sites. NHS Digital will be issuing guidance on unsupported systems in July 2017, and local organisations should be aiming to have isolated, moved away from, or be actively managing any unsupported systems by April 2018. We are working in partnership with Microsoft to help mitigate the immediate risks associated with unsupported software. NHS Digital will ensure that its CareCERT Assure on-site assessments looks at unsupported software and issue specific guidance on removing or isolating unsupported software. The Department of Health will also work with other Government Departments and NHS Digital to agree action to address key issues on unsupported software and technology. The CIO's review, to report by October 2017, will explore what further action is needed to address technology which risks the safe prioritisation of patient care, including diagnostic pathways.

11. **NHS England and NHS Improvement will lead a communications, engagement and training programme,** recognising the critical role that local leadership plays in an organisation's cyber resilience, a core message highlighted in last year's independent reviews. A network of 'cyber champions' will provide local support. We will support the primary care community to meet the 10 data security standards by ensuring that changes to GP systems provide essential data security by default, and work with professional associations and local government to provide guidance and information for health and social care professionals.

12. **To build local performance and boost capability**, NHS Digital has established the CareCERT suite of services, supporting health and care organisations to secure their own cyber resilience and respond to cyber incidents. NHS Digital has already produced and is testing the alpha version of the redesigned Information Governance Toolkit, as recommended by the NDG and CQC reviews, centred on assuring local implementation of the NDG's 10 data security standards. The new Information Governance Toolkit will be in place by April 2018 and will incentivise organisations to report near misses. The NHS Digital is also boosting its capacity to support system network monitoring, alerts, on-site assessments to assess local cyber vulnerabilities and prioritise local mitigating action, based around implementation of the data security standards. NHS Digital is prioritising CareCERT on-site assessments, by October 2017, for those NHS Trusts affected by the May 2017 ransomware incident.

13. **Improving threat surveillance and incident response is critical.** The Department of Health is working with the NCSC, NHS England and NHS Digital to prepare and rehearse incident response plans and take action to strengthen communications when core computer systems go down.

Implementing an opt-out to support patient choice about how their confidential data is shared

14. The health and social care system's ability to use technology and patient data effectively and efficiently is integral to transforming care, delivering sustained improvement and innovation in service delivery and supporting medical research with the aim of improving patient experience and outcomes and reducing health inequalities.

15. We want to encourage the public to share their data with the health and social care system in the knowledge that it is used appropriately and lawfully, and is held securely.

16. To achieve this we will:

- Implement the national opt-out.
- Protect and share anonymised information.
- Improve people's understanding of how their data has been used.
- Provide clarity on how data is shared lawfully and safely for direct care.

17. We will work collaboratively with patients, professionals and stakeholders to implement the national opt-out and test and refine our approach to take account of people's feedback.

18. **Implementing the national opt-out**

- **NHS Digital and NHS England** will engage with professionals and the public including developing guidance to highlight how patient data is kept safe and used to benefit the health and social care system and for research. NHS Digital will develop, test and prepare for introducing the national opt-out with all stakeholders. The public will be able to start choosing if they wish to opt out nationally from March 2018. Existing opt out will be respected until 2020 and the NDG will be consulted before their removal.

19. **Sharing and protecting anonymised information**

- **NHS Digital** will work with GP professional organisations and GP systems suppliers to look at how patient data can be de-identified on collection from GP practices. This will be introduced from September 2019. It will build on work by the Information Governance Alliance (IGA) and Information Commissioner's Office (ICO) on protecting anonymised data.

20. We will work with stakeholders during implementation to ensure that the national opt-out is introduced to best enable the health and social care system to access the data it needs.

21. **Improving transparency for the public** about how and why their information has been used for health and care purposes, and the benefits this has had will be key to successfully implementing the national opt-out, and changing culture and behaviour around data sharing. By September 2017, NHS Digital's data release register will set out the benefits of how data released by NHS Digital has been used, in a way that is easy for the public to understand. By December 2018, individuals will be able to access a digital system to understand who has accessed their summary care record and, by March 2020, they will be able to see who has used their data collected by NHS Digital.

Implementation plan on data security and data sharing

A. Overarching	
Department of Health: Publish the Government response to the NDG and CQC reviews, with the formal acceptance of the 10 data security standards.	July 2017.
B. Establishing a clear contractual and regulatory framework	
NHS England: Include NDG standards and recommendations in the NHS Standard Contract	Standards and recommendations included in the NHS Standard Contract since 1 April 2017.
NHS Improvement and CQC: ensure that organisations are implementing the 10 data security standards, and that this is considered in decisions to apply regulatory powers.	i. New CQC inspection framework for Trusts published June 2017 – Develop interim CQC tools / guidance – July to September 2017 ii. Interim CQC inspection approach, implemented for: – NHS Trusts – from September 2017 – NHS GPs and adult social care providers – November 2017 iii. Updated CQC inspection approach developed and rolled out from April 2018.
NHS England and NHS Improvement: start following up critical CareCERT alerts, reported through the CareCERT Collect system within 48 hours to confirm that local organisations have the necessary plans in place.	Summer 2017 [Full roll out. This has already been rolled out across major trauma units and Ambulance Trusts].
NHS Improvement: publish the 'statement of requirements', used to underpin the data security standards and the NHS Standard Contract requirements, to clarify required action for local organisations - including the requirement for a named executive Board member responsible for data and cyber security - and also ensure that Chief Executive Officers confirm in an annual 'statement of resilience' the actions they are taking to meet those requirements.	Summer 2017.

The **Network and Information Systems Directive** will give further legal backing to the data security standards by requiring those organisations identified as 'operators of essential services' to comply with defined security requirements.	May 2018.
C. Addressing infrastructure weaknesses	
NHS England and NHS Improvement: Implement the initial £21 million capital funding for 2017/18 to increase cyber resilience and address structural weaknesses of major trauma centres.	Immediate investment in the 2017/18 financial year.
NHS Digital: Look at unsupported software as part of CareCERT Assure on-site assessments. Issue guidance on removing or isolating unsupported software.	Guidance to be published July 2017.
Department of Health, working with other Government Departments and NHS Digital to agree action to address key issues on unsupported software and technology.	Framework in place to support organisations to move to the latest operating system by March 2018.
Chief Information Officer for health and care's review: explore what further action is needed to address technology which risks the safe prioritisation of patient care, including diagnostic pathways.	By autumn 2017.
D. Communications and engagement	
NHS England and NHS Improvement to lead a coordinated engagement programme - recognising the critical role that local leadership plays in an organisation's cyber resilience.	July 2017 to end March 2018.
NHS Digital to lead a communications campaign on the importance of data security at a clinical, administrative and technical level in the health and social care system.	July 2017 to end March 2018.

NHS England to establish regional cyber champions to provide local support.	December 2017.
E. Building local performance and boosting capability	
NHS Digital: prioritising on-site vulnerability assessments for the 47 Trusts affected by the May 2017 ransomware incident. **NHS Digital** also boosting its capacity to support the system through alerts and on-site assessments which will assess local cyber vulnerabilities and prioritise local mitigating action, based around implementation of the data security standards.	60 NHS Trusts and Foundation Trusts have already undergone an on-site assessment. Second phase of CareCERT Assure assessments complete by January 2018.
Department of Health and NHS Digital: design and test the proposed framework for measuring progress in implementing the data security standards which will be implemented through the revised Information Governance Toolkit.	Testing with organisations already completed. The proposed measurement framework will be published in summer 2017.
NHS Digital: redesign Information Governance Toolkit to provide the tool for measuring progress in line with the measurement framework.	By April 2018.
F. Improving threat surveillance and incident response	
Boosting **NHS Digital's** capacity to support system network monitoring to identify cyber vulnerabilities and prioritise mitigating action.	i. CareCERT monitoring capability across the national network was established in 2015. ii. An enhanced National Monitoring Security Operations Centre is in progress and due to deliver in March 2018, together with a phased plan for further developments to meet system needs.

Implementing an opt-out to support patient choice about how their data is shared

G. **Implementing a simplified national opt-out** Making it clear to the public and professionals how personal health and care data is used, how privacy is protected, and the choices available to people under the national opt-out.	
NHS England and NHS Digital will engage with professionals and patients to develop communications and guidance to support professionals, practitioners and frontline staff implement the national opt-out.	From July 2017.
NHS England, NHS Digital and other partners will put plans in place to better communicate to the public how data is protected, safeguarded and used, the benefits of data sharing for research and to improve the running of the health and social care system.	From July 2017.
NHS Digital will work with partners, the public and professionals to develop, test and introduce the ability for the public to set a national opt-out digitally and non-digitally:	
• The national opt-out service will be tested with the public and professionals.	From September 2017.
• The health and care service including GP Practices will be readied for public launch.	From October 2017.
• Changes will be communicated to patients who have set existing type 2 preferences.	From January 2018.
• Nationally, members of the public will be able to start setting national opt-outs.	From March 2018.
Department of Health will work with **NHS England** and **NHS Digital** to ensure all health and social care organisations are upholding the national opt-out.	By March 2020.

The health and social care system will respect existing type 1 opt-outs until 2020. The **Department of Health** will consult with the National Data Guardian in March 2020 before their removal.	By March 2020.
H. Sharing and protecting anonymised information	
NHS Digital to implement a new mechanism to de-identify data on collection from GP Practices.	From September 2019.
Information Governance Alliance to develop and consult on guidance setting out how the health and social care system should meet the ICO Code of Practice on Anonymisation.	2018.
The Government will implement UK data protection legislation to provide a strengthened legal framework for protecting personal data.	By May 2018.
I. Audit and transparency: improving people's understanding about how their data has been used NHS Digital will make it easier for patients to access and understand how their data has been used nationally. This will be achieved by working with patients to understand what they need, and using improvements in available technology and systems.	
The data release register, published by **NHS Digital**, will set out the benefits from how data released by NHS Digital has been used, in a way that is accessible to members of the public.	By September 2017.
Public will be able to access a digital service that enables them to see who has accessed their summary care record.	By December 2018.
Public will be able to use online services to see how their data, collected by NHS Digital, has been used for purposes other than for their direct care.	By March 2020.

J. Providing clarity on how data is shared lawfully and safely for direct care	
Department of Health will commission NHS Digital and NHS England to develop a framework on sharing data for direct care.	By July 2017.
To strengthen and formalise the role of the NDG further and to create Parliamentary accountability, we are working to put the NDG on a statutory footing.	2019.

Annex H: Glossary

Aggregated data: Statistical data about several individuals that has been combined to show general trends or values without identifying individuals within the data.

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

Caldicott Guardian: A senior person responsible for protecting the confidentiality of patients' and service-users' information and enabling appropriate information-sharing. Each NHS organisation is required to have a Caldicott Guardian with specific responsibilities to oversee an ongoing process of audit, improvement and control. This was mandated for the NHS by Health Service Circular: HSC 1999/012.

CareCERT: CareCERT offers advice and guidance to support health and social care organisations to respond effectively and safely to cyber security threats.

Chief Information Officer (CIO): An executive job title commonly given to the person at an enterprise in charge of information technology (IT) strategy and the computer systems required to support an enterprise's objectives and goals.

Commissioning (and commissioners): Buying care with available resources to ensure that services meet the needs of the population. The process of commissioning includes assessing the needs of the population, selecting service providers and ensuring that these services are safe, effective, people-centred and of high quality. Commissioners are responsible for commissioning services.

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 know 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 Caldicott2 for definitions of explicit and implied consent.

Cyber Essentials: Government-backed and industry supported scheme to guide businesses in protecting themselves against cyber threats.

Cyber threat: The possibility of a malicious attempt to damage or disrupt a computer network or system.

Data breach: Any failure to meet the requirements of the Data Protection Act, including but not limited to an unlawful disclosure or misuse of personal data.

Data controller: A person (either alone or jointly or in common with others) who determines the purposes for which and the manner in which any personal confidential data are or will be processed. A person in this context refers to a body with a legal identity and data controllers are usually organisations rather than individuals.

Data integrity: Property that reflects the fact that data have not been altered or destroyed in an unauthorised manner.

Data protection: Technical and social regimen for negotiating, managing and ensuring informational privacy, confidentiality and security.

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 quality: The correctness, timeliness, accuracy, completeness, relevance and accessibility that make data appropriate for their use.

Data security: Protecting data, such as a database, from destructive forces and from the unwanted actions of unauthorised users.

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.

Data sharing agreements/protocols: A common set of rules adopted by the various organisations involved in a data sharing operation.

Data subject: An individual who is the subject of personal data.

De-identified: This refers to personal confidential data, which has been through anonymisation in a manner conforming to the ICO Anonymisation code of practice. There are two categories of de-identified data:

- De-identified data for limited access: this is deemed to have a high risk of re-identification if published, but a low risk if held in an accredited safe haven and subject to contractual protection to prevent re-identification;
- Anonymised data for publication: this is deemed to have a low risk of re-identification, enabling publication.

Direct care: 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, 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.

Disclose/Disclosure: The act of making data available to one or more third parties.

Disclosure control: Assessing the risk of disclosure from a potential release and taking measures, if appropriate, to lower that risk.

Encryption: The process of transforming information (referred to as ‘plain text’ or ‘in the clear’) using an algorithm (called a ‘cipher’) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a ‘key’.

Genome: The total genetic complement of an individual.

ICO: The Information Commissioner’s Office, established as the UK’s independent authority to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Information Governance: The set of multidisciplinary structures, policies, procedures, processes and controls implemented to manage information at an enterprise level, supporting an organisation’s immediate and future regulatory, legal, risk, environmental and operational requirements.

Information Governance Toolkit: An online system which allows NHS and social care organisations to assess themselves or be assessed against Information Governance policies and standards. It also allows members of the public to view participating organisations’ IG Toolkit assessments.

Incident reporting: A method or means of documenting any unusual problem, occurrence, or other situation that is likely to lead to undesirable effects or that is not in accordance with established policies, procedures or practices.

Incident management: A term describing the activities of an organisation to identify, analyse and correct hazards to prevent a future re-occurrence.

ISO/IEC27000 series: Information security standards published jointly by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Linked data: The result of merging data from two or more sources with the object of consolidating facts concerning an individual or an event that are not available in any separate record.

Malware: An umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware and other malicious programs. It can take the form of executable code, scripts, active content and other software.

Opt-out: The option for an individual to choose not to allow their data to be used for the purposes described.

Personal Confidential Data (PCD): Personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of the NDG review ‘Personal’ includes the DPA definition of personal data, but it is adapted to include dead as well as living people and ‘confidential’ includes both information ‘given in confidence’ and ‘that which is owed a duty of confidence’ and is adapted to include ‘sensitive’ as defined in the Data Protection Act. The NDG review used the term “personal confidential data”, which was the term used in the second Caldicott report. The Government’s response uses the same term for consistency, though we accept that there are differing interpretations of this and that the commonly understood legal term is ‘confidential patient information’. The Wellcome Trust’s Understanding Patient Data initiative recognizes the language used to describe patient data is complex and confusing. It is important that we use the right words to describe what we mean which are understandable and meaningful to people. Understanding Patient Data has suggested ‘patient data’ and ‘patient health information’ as the most effective terms to use. We will give further consideration to this issue as we implement the recommendations of the NDG review and in particular the new opt out to ensure there is absolute clarity for the public.

Personal data: Data which relate to a living individual who can be identified from those data, or from those data and other information which are in the possession of, or are likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Pseudonym: Individuals distinguished in a data set by a unique identifier which does not reveal their 'real world' identity.

Pseudonymised data: Data that has been subject to a technique that replaces identifiers with a pseudonym. In practice, pseudonymisation is typically used with other anonymisation techniques.

Records Management: The practice of maintaining the records of an organisation from the time they are created up to their eventual disposal. This may include naming, version control, storing, tracking, securing and destruction (or in some cases, archival preservation) of records.

Re-identification: The process of analysing data or combining them with other data with the result that individuals become identifiable. This is also known as 'de-anonymisation'.

Safe Haven: An agreed set of administrative procedures and physical security to ensure the safety and secure handling of confidential patient information. Safe Havens were developed in the early 1990s to keep commissioning data secure and were often associated with a locked room with limited staff access.

Acknowledgements

The Department of Health would like to thank the following organisations for contributing the case studies to this response:

Alzheimer's Research UK

Alzheimer's Society

Association of Medical Research Charities

Asthma UK

British Orthopaedic Association

Derby City Council

Diabetes UK

Genomics England

Great Ormond Street Hospital

Kidney Research UK

Local Government Association

Macmillan Cancer Support

Multiple Sclerosis Society

Public Health England

Salford Lung Study

Southall and Brent Revisited (SABRE)

Stroke Association

The Richmond Group of Charities

Understanding Patient Data

Wellcome Trust

Yorkshire Cancer Research

Department
of Health

CCS0517428676-3 July 2017
Produced by APS Group for the Department of Health