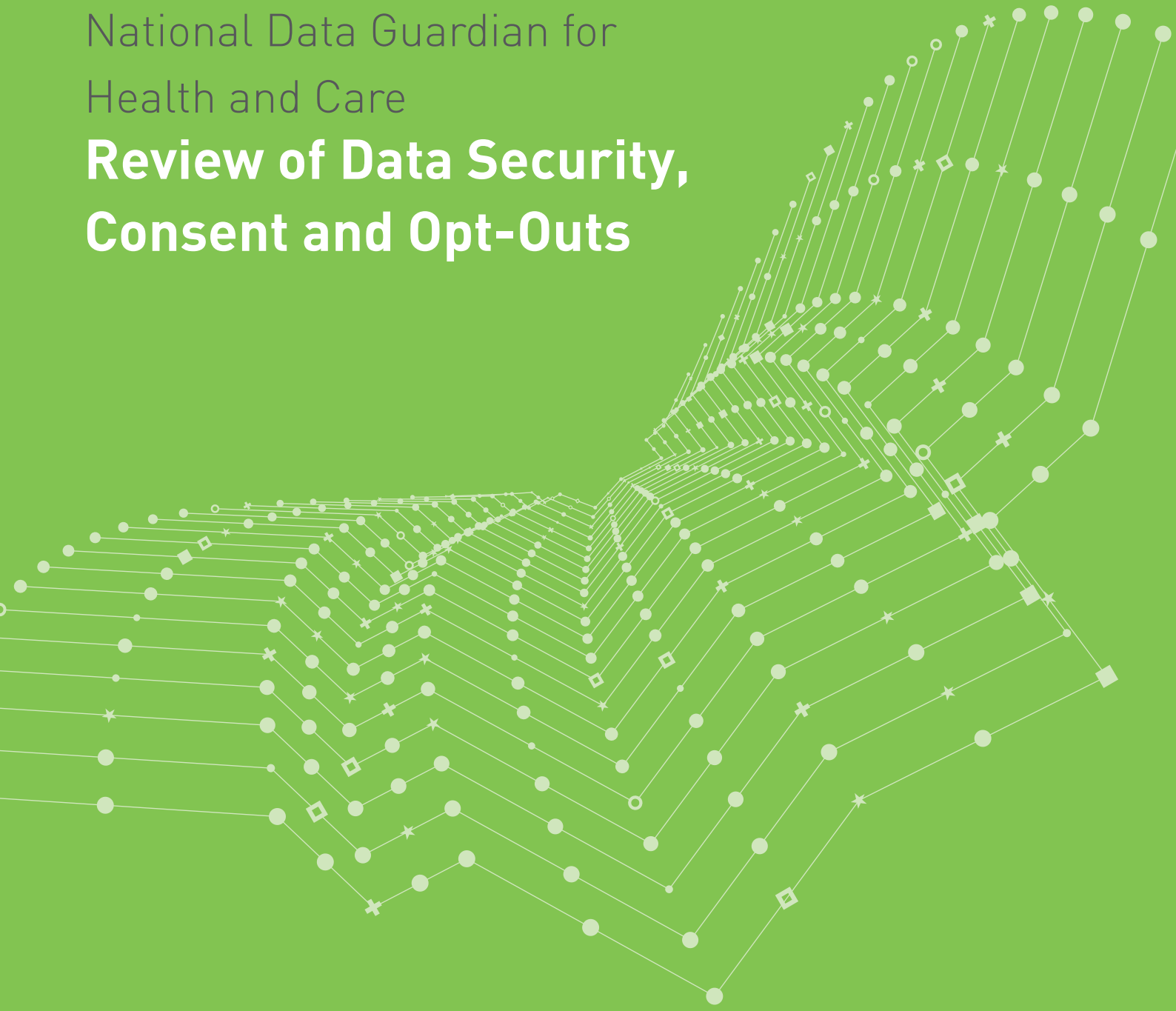
National Data Guardian for Health and Care

Review of Data Security, Consent and Opt-Outs



National Data Guardian

Contents

Foreword by Dame Fiona Caldicott

Everyone who uses health and care services should be able to trust that their personal confidential data is protected. People should be assured that those involved in their care, and in running and improving services, are using such information appropriately and only when absolutely necessary. Unfortunately trust in the use of personal confidential data has been eroded and steps need to be taken to demonstrate trustworthiness and ensure that the public can have confidence in the system.

At the beginning of September 2015, the Secretary of State for Health asked me, as the National Data Guardian, to work alongside the Care Quality Commission (CQC), and carry out an intensive Review to recommend: new data security standards, a method for testing compliance against these standards, and a new consent or opt-out model for data sharing in relation to patient confidential data.

This Review follows two previous reviews. In 1996-7, I chaired a Review on the use of patient identifiable data where we recommended six principles for the protection of people's confidentiality, which became known as the 'Caldicott principles'. In 2013, I led the Information Governance Review and we recommended an additional 'Caldicott principle' setting out that the duty to share information can be as important as the duty to protect patient confidentiality.

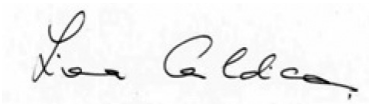
I agreed to undertake this third Review for two reasons. Firstly, there has been little positive change in the use of data across health and social care since the 2013 Review and this has been frustrating to see. Secondly, because I believe we have a very significant opportunity now to improve the use of data in people's interests, and ensure transparency for the public about when their data will be used and when they can opt out of such usage.

I have worked alongside CQC, which was asked to review the current approaches to data security in NHS organisations that provide services. Its work has been invaluable in developing an evidence base for the new data security standards which are set out in this report. The data security standards are intended to be applied across all health and social care organisations. Further work will be needed to establish the validity of the new data security standards for organisations providing social care, as this was not included in the CQC review.

Data security is also integral to the second part of this Review: designing a model for information-sharing. The trust needed for effective information-sharing cannot be ensured without secure systems and easily understood explanations of how information and privacy are protected. I have proposed a new consent/opt-out model that describes clearly when information is used, and when patients have a choice to opt out of their personal confidential data being used. The model does not supersede any of the existing Caldicott principles. Patients and service users should not be surprised that an appropriate professional has access to information about them when they seek care, and should be confident that only the minimum amount of information needed to provide that is shared.

I submitted this Review to the Government in March 2016. Since then I have taken the opportunity to update some references, but have not made any changes of substance.

It was a short Review and significant work will need to be undertaken to implement the recommendations, which should include a full and comprehensive public consultation. A key aspect of this work must be a dialogue with the public. We owe it to citizens to enable them to understand data usage as fully as they wish, and ensure that information about how data is accessed, by whom, and for what purposes, is available. This work is part of a wider dialogue that should be conducted on data use across different sectors. Health and social care data, although unique, cannot be isolated from that discussion.



Dame Fiona Caldicott, MA FRCP FRCPsych
National Data Guardian

June 2016

1. Overview

1.1 This is a report about trust. It addresses the question of what more can be done to build trust in how the NHS and social care services look after people's confidential data and use it appropriately.

1.2 Health and social care services have always depended on trust. People must feel able to discuss sensitive matters with a doctor, nurse or social worker without fear that their information may be improperly disclosed. People also expect that this confidential information will be shared with other professionals in the care teams supporting them. Now, as health and social care become increasingly integrated, and as more data is held on computers (and computers are becoming more powerful), it is becoming ever more important that people understand when and how information is shared, how privacy is protected, and how sharing information benefits them and others.

1.3 This report focuses particularly on two aspects of people's trust. Firstly, it looks at whether data security is good enough. Are there adequate systems in place to prevent people's confidential information falling into the wrong hands? Can those systems be made strong enough to protect against known and potential dangers without being so restrictive that information cannot be shared appropriately among staff providing care? Secondly, the report looks at the basis upon which information is shared. Do people understand who will have legitimate access to their personal confidential data? When is the individual's specific consent required? When can people consent to or opt out from information being used and when may this be overruled? Are the current arrangements protecting people's confidentiality adequately upheld, and do they allow for appropriate information sharing to benefit patients, service users and the entire health and care system?

Origin of the Review

1.4 In a speech to the NHS Innovation Expo in Manchester on 2 September 2015, the Secretary of State for Health challenged the NHS to make better use of technology. His proposals included rapid progress in the arrangements for patients to access and add to their own electronic health records. Technology will also permit health and social care professionals across England to share life-saving information about individuals, whenever and wherever they need attention. The Secretary of State said: 'Exciting though this all is, we will throw away these opportunities if the public do not believe they can trust us to look after their personal medical data securely. The NHS has not yet won the public's trust in an area that is vital for the future of patient care'[1].

1.5 To address this issue, he commissioned a Review of data security and consent and asked for the Review to report in January 2016. Firstly, he asked the Care Quality Commission (CQC) to review current approaches to data security across the NHS to prevent personal confidential data falling into the wrong hands. Secondly, he asked Dame Fiona Caldicott, the National Data Guardian (NDG), to develop data security standards that can be applied to the whole health and social care system and, with CQC, devise a method of testing compliance with the new standards. Thirdly, he asked Dame Fiona to propose a new consent/opt-out model for data sharing to enable people to make an informed decision about how their personal confidential data will be used[2].

1.6 This report provides the results of the two pieces of work undertaken by the NDG. It provides details of the evidence found by the NDG's Review, sets out new data security standards and recommendations for embedding those in organisations, and proposes a new opt-out for information sharing. The recommendations are being made to the Secretary of State for Health, and the NDG recommends that the Department of Health conducts a comprehensive formal consultation on the proposed standards and consent/opt-out model. The Review has been conducted within a tight schedule. Because of this, work will be needed to sufficiently prepare and explain the recommendations to the public and professionals before implementation. Even so, the Review team has been mindful of the importance of getting the

1. Secretary of State for Health Speech at NHS Innovation Expo, September 2015
2. Annex A National Data Guardian's Review Terms of Reference

recommendations as right as possible in the time available.

Evidence and analysis

1.7 The Review conducted a series of evidence sessions and interviews with key organisations and stakeholders, including patient representative groups, GPs and other clinicians, commissioners and providers of health and social care services, researchers and the Information Commissioner's Office (ICO). Written evidence was also accepted.

1.8 In relation to security, the Review met with the providers of IT systems to GP surgeries and social care, and data security experts. Alongside this, CQC commissioned 120 days of fieldwork in 60 GP practices, NHS Trusts, and dental surgeries, and in total interviewed over 200 NHS staff.

1.9 Specifically in relation to information sharing and consent, the Review carried out eight focus groups with members of the public across the country and an online survey of over 400 patients and service users. Recognising that the interests of patients and service users are at the heart of the Review, an analysis of existing evidence on public opinion was undertaken and compared to the findings from the eight public focus groups. The Review used the evidence to develop its recommendations and model. These were explored with patients, service users and health and social care professionals in Lancaster, Leeds, London and Hampshire. Workshops were also held with local Healthwatch representatives and with members of the public (including jointly with the Cabinet Office Policy Lab) to test and refine the model.

Data security

1.10 The evidence shows that people trust the NHS to protect information. However, there are cases where that trust has been eroded by data breaches, such as when emails containing sensitive information have been sent to the wrong address, data is shared without consent, or people experience their records being misplaced or lost.

1.11 Whilst there are examples of good practice and most organisations are concerned about data security, there are problems involving people, processes and technology. Data is not always adequately protected and individuals and organisations are not consistently held to account. Examples of poor practice include confidential papers being stored in unlockable cabinets, faxes being sent to the wrong number and the use of unencrypted laptops. As the health and social care system becomes increasingly paperless and digital, many of these issues will be addressed automatically.

1.12 Leadership is crucial. Where the Senior Information Risk Owner's (SIRO) responsibility is only one part of someone's job, and not prioritised, data security can suffer. As patient data becomes increasingly digital and computers become the sole means of obtaining critical information (such as that relating to allergies or blood types), the integrity and availability of data are increasingly linked to the quality and safety of care. People's confidential data should be treated with the same respect as their care.

1.13 Personal confidential data is valuable to those with malicious intent, and health and social care systems will continue to be at risk of external threats and potential breaches. However, internally, data breaches are often caused by people who are finding workarounds to burdensome processes and outdated technology, and may have a lack of awareness of their responsibilities. A strong SIRO and an engaged board can make a significant difference, and where properly supported the appointment of Caldicott Guardians has had a positive impact. GPs and social care professionals want a simple explanation of what they should and should not be doing and reassurance that partner organisations are protecting personal confidential data. Better technology, and the move to a paper-free NHS, are seen as important in helping people to do the right thing. There is widespread appreciation of the need for digital systems, but concern that the move to digitally stored personal confidential data will increase the impact on organisations and individuals of any breaches.

Data security standards

1.14 Data security frameworks, assurance schemes and standards already exist. They include: the Information Governance Toolkit (IG Toolkit), the Cyber Essentials Scheme, the 10 Steps to Cyber Security, and the ISO/IEC27000 series. The IG Toolkit has often been seen as a tick-box exercise, while the Cyber Essentials scheme is not yet widely used in health and social care. Meanwhile, the ISO standards are generally regarded as too expensive and time-consuming to be applied broadly in this sector.

1.15 The NDG recommends new data security standards for every organisation handling health and social care information. These have been designed to

be simple for people to understand and follow. They should apply across the entire health and social care system and are intended to support rather than inhibit data sharing. These standards have also been designed to be fit for the future, where personal confidential data will be stored digitally rather than in filing cabinets, and health and social care will be integrated. The standards are designed to address the principal root cause of existing breaches to security of paper-based and digital data, and to protect systems against potential future breaches to digital data.

Embedding the data security standards

1.16 Properly trained and well-motivated staff are essential. The Information Governance Toolkit should be updated to support and underpin the new standards. Annual role-appropriate training should be mandatory for all who work in health and social care, with bespoke additional training for people in leadership roles, such as Caldicott Guardians, SIROs and board members. Trusts and Clinical Commissioning Groups (CCGs) should use appropriate tools to identify unused and dormant accounts, unsupported systems and software, poorly maintained access permissions or default passwords. To support risk assessment activities, organisational leaders should refer to central sources such as CareCERT, the Health and Social Care Information Centre (HSCIC)[3] and the National Technical Authority for Information Assurance (CESG) for information about potential threats. Action should be taken immediately following a data breach or near miss, with a report to senior management within 12 hours. There must be a culture of learning from, and not blaming over security breaches.

1.17 The new standards should be embedded in the health and social care system with organisations providing objective assurance about how they have complied with them. 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 IG Toolkit to inform CQC of 'at risk' organisations, and CQC should use this information to prioritise action. Finally, there should be much tougher sanctions for malicious or intentional data security breaches.

Consent and opt-outs

1.18 When commissioning this Review, the Secretary of State said: 'I would like you to develop a single question consent model which makes it absolutely clear to patients/users of care when health and care information about them will be used and in what circumstances they can opt out.' The Review started this aspect of its work by considering what lay behind the Secretary of State's request for greater clarity.

1.19 Data sharing is essential for high quality health and care services. It is integral to identifying poor care; it is clear that more effective data sharing could have enabled some of the recent failures to provide proper care to patients to be identified and tackled earlier. People provide the professionals who are caring for them with their personal confidential information, without which the care would not be effective or safe. There can be no doubt that such information, drawn from millions of people, can be extremely useful for other purposes, such as medical research, planning better services and ensuring that NHS and social care organisations invoice each other for the correct amounts when necessary. But when patients and service users provide their information to a care professional, they cannot be expected to know all the other uses to which it may be put. There are laws to prevent improper disclosure and procedures to ensure that permission for such 'secondary use' is limited, ethical and secure. However, the laws and procedures are difficult for the experts to understand, let alone the patients and service users. It is hard to argue that patients and service users have consented to uses of their personal confidential information that they cannot anticipate, according to procedures that they cannot understand. This issue is particularly troubling for individuals who have strong views about how their information may be used.

1.20 Patients and service users who are concerned about this problem are given reassurance in the NHS Constitution, which says: 'You have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis.' However, the NHS Constitution does not provide an absolute right to stop confidential information flowing and it does not apply to social care.

1.21 On 26 April 2013, the Secretary of State for Health gave a stronger form of reassurance. In a statement of policy, he said that any patient who did

3. On 20 April 2016, George Freeman, Minister for Life Sciences, announced that the Health and Social Care Information Centre would change its name to NHS Digital. The name change is to take effect from 1 August 2016. This decision chimes well with Recommendation 12 of this Report in paragraph 3.2.31. However, the Review makes frequent reference to work done by the HSCIC before the renaming. To avoid confusion, this report refers to HSCIC throughout.

not want personal data held in their GP record to be shared with the Health and Social Care Information Centre (HSCIC) would have their objection respected. On 12 September 2013, he added: 'All they have to do in that case is speak to their GP and their information won't leave the GP surgery'. This became known as a 'Type 1' objection. The Secretary of State was speaking at the launch of the HSCIC publication, 'A guide to confidentiality in health and social care' which gave patients further assurance. As well as objecting to confidential information about them being sent from a GP practice, patients would be able to tell their GP if they objected to any confidential information about them leaving the HSCIC in identifiable form. This applied to personal confidential data received by HSCIC from all sources, not just GPs. It became known as a 'Type 2' objection.

1.22 These new rights to object were communicated to patients in a leaflet from NHS England for every household in January 2014. The leaflet[4] explained that the NHS would extract data from GP records and combine it with other data from hospital records. It described how this information would be used to improve patient care, and explained the choices available to patients. The care.data programme, which was due to start extraction in spring 2014, was paused on 18 February 2014 after criticism from the Royal College of General Practitioners, the British Medical Association, Healthwatch England and others. It is against the background of this complexity that the Secretary of State asked for the Review to develop a simple consent/opt-out model that people could more easily understand.

Public views

1.23 On data sharing and opt-outs, public views have not changed very much since the 2013 Information Governance Review[5], known as Caldicott2. People accept that their information will be used to support their own care and find it frustrating when they have to repeat their information to different health and social care professionals. However, people hold mixed views about their information being used for purposes beyond direct care. Some are concerned primarily with privacy and are suspicious that information might be used by commercial companies for marketing or insurance. Others prioritise the sharing of information to improve health and social care, and for research into new treatments. There is broad support for data being used in running the health and social care system when the benefits of doing so are clearly explained, but people think that anonymised information should be used wherever possible. The Review also heard very strong views from providers, commissioners, researchers and public bodies that high quality person-level data is needed to run the health and social care system, and to support research.

1.24 It is clear that people do not fully understand what options they have in relation to the use of their information, and find the current system difficult to understand. Likewise many health and social care professionals lack confidence in what they are allowed to do with personal confidential data and what can be shared with whom. As health and social care services move towards greater integration and collaboration, this uncertainty is creating barriers to the improvement of services.

The new consent/opt-out model

1.25 The National Data Guardian recommends a new consent/opt-out model to give people a clear choice about how their personal confidential data is used for purposes beyond their direct care. This has been developed through close working with professionals, including the Royal College of General Practitioners (GPs), the British Medical Association, the Information Commissioner's Office, the Local Government Association, research organisations and charities. Input was also provided on iterative versions of the model by GPs, social care professionals, as well as patients and service user groups in Lancaster, Leeds, West Hampshire and London.

1.26 Information is essential for high quality health and care, to support the provision of excellent care and for the running of the health and social care system. It is also essential to improve the safety of care, including through research, to protect public health, and support innovation. It can be beneficial to join health data with other types of information, to provide better services to people. However, the case for data sharing still needs to be made to the public. All health and social care, research and public organisations should share responsibility for making that case.

1.27 The Review considered the personal confidential data needed for commissioning, public health, research and monitoring services. Strong cases can be made for sharing information, e.g. in planning healthcare, and for medical research. The Review heard that personal confidential data is essential to some specific purposes. It also heard differing views

4. https://www.england.nhs.uk/wp-content/uploads/2014/01/cd-leaflet-01-14.pdf
5. "To Share Or Not To Share? The Information Governance Review" https://www.gov.uk/government/publications/the-information-governance-review

about whether people should be given an opt-out from these purposes. Because of the importance of earning public trust, the Review concluded that people should be able to opt out of their personal confidential data being used for purposes beyond their direct care unless there is a mandatory legal requirement or an overriding public interest.

1.28 **The Review proposes that people should be able to opt out from personal confidential data being used beyond their own direct care**.

1.29 The proposed consent/opt-out model would apply to purposes other than direct care. Data should only be used where there is a clear legal basis. An individual choosing to opt out would stop access to her or his data for those purposes. The Review considered whether people should have a single choice about whether to opt out, or whether their choice should be split into two parts. The two-part approach would allow an individual to opt out of her or his data being used for purposes connected with providing local services and running the NHS and social care system. In a separate decision, the individual would be able to opt out of her or his data being used to support research and improve treatment and care. Individuals should be able to give their consent for defined uses such as a specific research project, as they do now.

1.30 **The Review recommends that the proposed consent/opt-out model should be put out to consultation. It is recommended that alongside the consultation there should be further testing to find out whether people would prefer to have more than one choice, and to develop the wording of the question.**

1.31 The new model should be implemented by all organisations that use health and social care information. Ultimately, a patient should be able to state their preference once (online or in person), confident in the knowledge that this will be applied across the health and social care system. They should be able to change their minds if they wish, and this new preference should be honoured. This would mark a significant step forward in allowing patients to understand and shape the use of their health and social care information.

1.32 The new model will not change the current system with regard to sharing for direct care. Relevant information about a patient should continue to be shared between health professionals in support of their care. An individual will still be able to ask their doctor or other healthcare professional not to share a particular piece of information with others involved in providing their care and should be asked for their explicit consent before access to their whole record is given. Similarly, health and social care integration has been driving local innovation in services which rely on (appropriate and legal) sharing of personal confidential data. Different parts of the country have already put arrangements in place to help people to understand how their data is being used to support care such as the Leeds Care Record, and the North West London Integrated Care Pioneer. In recognition of the value of these local innovations, the Review has sought to develop a solution that complements rather than conflicts with what is being achieved locally.

1.33 The new model will also not change the current system with regard to people's ability to give specific explicit consent to participate in research projects. People have always been able to choose to participate in research studies, such as UK Biobank, in which 500,000 people have chosen to help researchers discover why some people develop particular diseases and other people do not.

1.34 The Review heard that de-identified[6] data is of considerable benefit to commissioners, planners and researchers and that the public is broadly content for such information to be used for health and social care purposes. The Review strongly encourages organisations to continue exploring where de-identified and anonymised data that meets the Information Commissioner's Office Anonymisation Code of Practice may be used rather than personal confidential data. The Review proposes that data should be passed to the HSCIC, as the statutory safe haven of the health and social care system, to de-identify or anonymise and share it with those that need to use it. The Review notes the Government's decision to change the name of HSCIC to NHS Digital. This will provide that organisation with a good opportunity to use the NHS brand to make it clear to everyone that it is part of the NHS 'family'.

1.35 The Review considered whether people choosing to opt out should have their data withheld from this de-identification process. However, NHS and social care organisations are more likely to use de-identified and anonymised data if they can be confident that it is of high quality and provides the complete dataset. For that reason the Review recommends that, in due course, the opt-out should not apply to all flows of information into the HSCIC. This requires careful consideration with the primary care community,

6. See Annex G. Summary of Terms

which largely holds its responsibility as data controller dear, and with the public. It would, however, enable commissioners, for example, to fulfil many duties currently subject to Confidentiality Advisory Group (CAG) recommendations, without requiring access to personal confidential data. For the time being the status quo should prevail.

1.36 The Review considers that the Secretary of State's objective of creating a trustworthy system with the minimum use of people's personal confidential data would be better achieved by allowing all data to flow into the HSCIC. This would allow the HSCIC to link and then de-identify personal confidential data to create comprehensive de-identified data sets. For example, the Review heard evidence that information identifying individuals is currently used to look at groups of patients to show patterns where certain treatments are effective. However, if commissioners were provided with high-quality linked and de-identified data for such indirect care purposes, this could enable them to move away from using personal confidential data for these tasks.

1.37 The Review would like to see the good practice advice in the ICO's Anonymisation Code used as the minimum standard to safeguard all de-identified data which is to be used for health and social care purposes. The code explains the implications of anonymising personal data in accordance with the Data Protection Act (DPA)[7]. It contains, in full, the Information Commissioner's recommendations about anonymising personal data and assessing the risks associated with producing, and particularly publishing, anonymised data. The Code provides advice on how to anonymise personal data so that individuals' privacy is not compromised by an inappropriate disclosure of personal data through re-identification. The ICO has the powers to issue monetary penalty notices of up to £500,000 for serious breaches of the DPA.

1.38 The combination of recognised national guidance for anonymisation alongside severe penalties for serious breaches of the DPA enable the Review to propose that data that has been de-identified according to the ICO's anonymisation code should not be subject to the opt-out. **In addition, it is clear that there is considerable public support for use of anonymised data and that this will provide an impetus for organisations to move away from using personal confidential data**. The Review recommends that the Government should consider introducing stronger sanctions to protect anonymised data. This should include criminal penalties for deliberate and negligent re-identification of individuals.

1.39 At the moment, there are a number of different opt-outs, including Type 1 and Type 2 opt-outs and other objections and opt-outs housed in national and local computer systems. The Review is not recommending any changes to the existing arrangements until there has been a full consultation on the proposed new consent/opt-out model. People have told the review they want a simple explanation and choices that are clearer to understand. The Review is proposing a new model that has been designed to provide that simpler and less complex approach. The HSCIC, as the statutory safe haven of the health and social care system, can share data securely, and the public can have confidence in a simpler model. Once the consultation is complete, and the new model is in place, the existing arrangements should be replaced. As part of managing this transition, the Department of Health should make sure it considers how to manage the objections already registered by patients both locally and nationally.

1.40 This Review was not asked to look at care.data, although the pathfinder areas have been involved in shaping and testing the proposed consent/opt-out model, as have vanguards and health and social care integration pioneers. The consent and opt-out models proposed by the Review go further than the approach that was planned for the pathfinder areas, and should replace the approach that had been developed for those areas. In the light of the Review, the Government should consider the future of the care.data programme.

Next steps

1.41 This has been a short Review, which has made significant efforts to take account of relevant evidence and involve as many people and organisations as possible. It has not been possible to address every issue in detail. For that reason the Review recommends that the Department of Health conducts a formal, full and comprehensive public consultation on the draft standards and the proposed consent/opt-out model, with testing alongside consultation of whether there should be one or two questions, and that specific work is done to look at the application of the data security standards in social care. There should be ongoing work under the National Information Board's leadership to look at the outcome of this consultation, how to continue to build public trust and how the consent/opt-out model can be implemented in a way which enables all those involved in health and social

7. ICO's Anonymisation Code https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

care to collectively support understanding of how information is shared, and the increasing benefit that it can bring to citizens. Professional bodies and patient representative groups should be further involved in testing and refining the potential opt-out.

1.42 Alongside this important engagement with patients and services users, it is also imperative that organisations whose work would be affected by the Review's proposals have the chance to respond to the recommendations during the consultation and are supported to prepare for implementation. Such groups include GPs and other care providers, NHS and Local Authority commissioners, and researchers.

Recommendations

1.43 The 2013 Information Governance Review, known as Caldicott2, made a series of recommendations which still hold good today. These included the need for boards and leaders to actively ensure that their organisation is competent in information governance practice, the inclusion of information governance as a core part of training and continuous professional development, and recommended actions to ensure the effective regulation of organisations' use of personal confidential data. The 2013 Review also recommended a list of actions to set out how redress for mistakes should be managed by every organisation in the health and social care system in England.

1.44 In January 2015, Dame Fiona Caldicott and her advisory panel published a report[8] examining the first year of implementation of the 2013 recommendations. This report recommended that individuals must be able to opt out of data sharing arrangements and be confident that their wishes are being respected consistently across the system. With respect to data security and consent, the Review builds on these two reports and makes the following recommendations:

Data security

Recommendation 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.

Recommendation 2: A redesigned IG Toolkit should embed the new standards, identify exemplar organisations to enable peer support and cascade lessons learned. Leaders should use the IG Toolkit to engage staff and build professional capability, with support from national workforce organisations and professional bodies.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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 IG Toolkit to inform CQC of 'at risk' organisations, and CQC should use this information to prioritise action.

Recommendation 8: HSCIC should work with the primary care community to ensure that the redesigned IG 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 care system.

Recommendation 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.

8. To share or not to share – The Independent Information Governance Oversight Panel's report to the Secretary of State for Health

Consent/opt-out

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 14: The forthcoming Information Governance Alliance'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 Anonymisation Code of Practice by re-identifying individuals.

Recommendation 15: People should continue to be able to give their explicit consent, for example to be involved in research.

Recommendation 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.

Recommendation 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.

Recommendation 18: The Health and Social Care Information Centre (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.

Next steps

Recommendation 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.

Recommendation 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.

2. Data security standards for health and social care

2.1. Summary of evidence and analysis

The public view

2.1.1 **The evidence shows that there is a high degree of public trust in the NHS's safeguarding of people's data[9], although that trust has been eroded by data breaches[10].** Such breaches include the accidental disclosure of the clinic list of email addresses at a HIV clinic[11], and by data sharing without consent, such as the Pharmacy 2U incident[12].

2.1.2 The patient focus groups found that the public needs reassurance about data security when data is moving outside the NHS. The Review heard that members of the public would also be reassured by implementation of secure measures such as a system that conforms to the highest independent standards of data security. The public would be reassured if organisations were assessed regularly for compliance against standards and if they comply with all legal requirements, with compliance processes strictly enforced[13].

2.1.3 There was a view expressed that some people would feel more confident about organisations handling their personal confidential data if harsher sanctions were in place for those found to have intentionally or maliciously breached data security[14].

The professional view

2.1.4 The Review also took evidence from providers and commissioners, the Information Commissioner's Office, frontline care staff, industry experts and professionals. Strong leadership was considered essential to effective data security[15] – a strong SIRO, an engaged Board and an effective Caldicott Guardian were cited as being essential to the success of the most well-governed organisations. However, the Review heard that there was concern that some board members would assume that data security was dealt with exclusively by the Caldicott Guardian or SIRO and therefore did not see data security as a collective board responsibility[16]. **GPs and social care professionals wanted a simple explanation of what they should and should not be doing and reassurance that partner organisations with whom they share data are protecting people's confidential data[17].**

Breaches

2.1.5 The Information Commissioner's Office led an evidence session as part of the Review to look at reported data breaches.

Information Commissioner's Office record of breaches

- In 2014/15, 41% of all breaches reported to the ICO were from the health sector.
- The number of breaches is rising, although the reasons for this are unclear.
- Breaches largely happened due to human behaviour.
- In 2014/15, 48% of data breaches in the health sector affected fewer than 10 data subjects, with only 9% affecting more than 1,000 data subjects (usually relating to spreadsheets).
- Technological issues also lead to breaches, such as unencrypted devices or information in supposedly anonymised data sets not being properly anonymised.
- The use of unencrypted devices is a concern across health and social care, resulting in a fine of £325,000 to a single NHS Trust.
- Across the health sector the ICO has issued 11 fines amounting to £1.4 million between April 2010 and November 2015.

9. Evidence heard at eight Patient Focus Groups which were held throughout October and November 2015 at different geographical locations throughout England (Referred to as 'Patient Focus Groups' hereafter)
10. Patients, Service Users and Carers Evidence Session, 24 November 2015
11. http://www.bbc.co.uk/news/uk-england-london-34127740
12. https://ico.org.uk/action-weve-taken/enforcement/pharmacy2u-ltd
13. Patient Focus Groups
14. Patients, Service Users and Carers Evidence Session, 24 November 2015
15. Information Commissioner's Office evidence session on security breaches, 6 November 2015
16. Interview with the Chief Executive & Deputy Director of Nursing, Royal College of Nursing, 25 November 2015
17. Information Commissioner's Office evidence session on security breaches, 6 November 2015

2.1.6 The Review heard firsthand accounts of cases where public trust has been eroded by data breaches, such as misplaced, lost or incomplete records[18]. Particular issues included the use of unencrypted devices, faxes being sent to incorrect numbers, ward handover sheets missing, and confidential papers being left on desks or stored in unlockable cabinets[19].

Technology

2.1.7 **Many of the information breaches historically reported by the health and social care sectors related to patient information on paper, or to technologies such as faxes. As the health and social care sector moves towards a paperless digital future, many of these issues will be addressed automatically**. Technology brings huge benefits: reducing the process burden on users, speeding up services and connecting disparate information to enable better quality of care. It also makes it possible to record every time that people's personal confidential data is accessed and used, allowing for audit so that correct processes can be enforced. However, technological advance has the effect of making the potential impact of breaches greater, both in terms of the quantity of people's data affected and the amount of information at risk. It is essential that the security benefits of technology are used to counteract the security risks that technology can bring.

The threat

2.1.8 **The Review heard that in most cases, breaches or cyber-attacks are unwittingly facilitated by the behaviour of employees who can be classed as 'non-malicious insiders', primarily motivated to get their job done and often working with ineffective technologies or processes**[20]. In an evidence session held with providers, the Review heard examples of agency nursing staff being unable to access the system unless the permanent staff logged in and left the application open for the use of the agency staff. This avoidance of correct processes was the only way they could treat patients in a timely manner using the technologies available to them[21].

2.1.9 **The Review heard that the external cyber threat was becoming a bigger consideration as systems become more digital**[22]**.** Beyond human error, the Review found that the main threat to the public and private sectors is from basic cyber-attacks, which use hacking tools that can be purchased readily and cheaply online and exploit publicly known vulnerabilities[23]. Recent observations report significant increases in the volumes and sophistication of unsolicited emails in global circulation, many containing 'malware' or hidden software, designed to cause harm, by exploiting unmanaged technical weaknesses and/or human naivety:

> *'Email traffic in Q1 2015 saw a considerable increase in the number of… spam… emails. For example, emails sent from the .work domains contained offers to carry out various types of work such as household maintenance, construction or equipment installation. Many of the messages from the .science domains were advertising schools that offer distance learning, colleges to train nurses, criminal lawyers and other professionals'*[24].

2.1.10 The HSCIC provided the following example report as evidence, detailing the number of different types of threats that were identified and blocked by their security systems over a number of weeks in Q3 2015-6.

18. Patients, Service Users and Carers Evidence Session, 24 November 2015
19. Information Commissioner's Office evidence session on security breaches, 6 November 2015
20. Interview with the Former Chairman of the Medical Ethics Committee & colleagues, British Medical Association, 23 November 2015
21. Provider Evidence Session, 27 November 2015
22. Interview with the Director of the Institute of Global Health Innovation at Imperial College London, 10 November 2015
23. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf
24. https://securelist.com/analysis/quarterly-spam-reports/69932/spam-and-phishing-in-the-first-quarter-of-2015/

Figure 1: Evidence of the threat of cyber-attacks submitted by the HSCIC

	Week number									
Threat type by calendar week	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**	**51**	**Total**
	2	6	2	2	3	1	46	7	20	89
	251	123	47	25	39	44	41	38	162	770
Total	**253**	**129**	**49**	**27**	**42**	**45**	**87**	**45**	**182**	**859**

2.2. Existing standards

2.2.1 A number of data security frameworks, assurance schemes and standards already exist and some aim to mitigate the threats outlined above. It was evident that there is no lack of guidance on good security processes – in fact, the Review heard that there may be too many pieces of guidance[25]. There was a call for standards to be simplified, with good practice championed so others can learn[26].

2.2.2 **The Review heard that data controllers were often confused by the plethora of data standards and good practice principles and unsure which guidance they should follow. There was also confusion about how legislation fits together and what takes precedence[27].** The Review heard that the self-assessment nature of existing compliance mechanisms such as the IG Toolkit was a concern[28], whilst audit and inspections were largely welcomed as an enforcement mechanism[29] to provide some 'teeth' in enforcement[30].

2.2.3 To understand the merits of and gaps within existing standards and assess whether they were appropriate, the Review Team carried out an analysis of existing data security standards (see Annex E for the full analysis). These included the IG Toolkit and Information Governance Statement of Compliance (IGSoC), CESG's Cyber Essentials, Cyber Essentials 'PLUS',10 Steps to Cyber Security, Cyber Streetwise website, and the Public Services Network – Code of Connection (PSN CoCo) operated by Government Digital Services (GDS). Commercially available standards operating within the wider public and private sectors were also considered, including the internationally recognised ISO/IEC27000:2013 series of Information Security Management standards and the Information Security Forum's Standards of Good Practice (ISF SoGP). The boxes below highlight some of the key standards.

2.2.4 The analysis of current standards operating within the health and social care sector suggested that whilst ISO/IEC 27001 and the ISF's Standards of Good

The Information Governance Toolkit: The mandatory policy delivery tool for data security

Use of the Information Governance Toolkit (IG Toolkit) is mandatory for NHS organisations and network service providers wishing to operate over the N3 network. The IG Toolkit is commonly used in health organisations, but uptake in social care is lower. The Review found that the IG Toolkit is well understood and well embedded across the health sector, but the Review heard evidence, in particular at the evidence session held for providers, that the self-assessment nature of the IG Toolkit causes some to doubt its reliability. It can be seen as a lengthy tick-box exercise.

25. Information Commissioner's Office evidence session on security breaches, 6 November 2015
26. Commercial Providers Evidence Session, 18 November 2015
27. Information Commissioner's Office evidence session on security breaches, 6 November 2015
28. Commercial Providers Evidence Session, 18 November 2015
29. Provider Evidence session, 27 November 2015
30. Interview with the Director of the Institute of Global Health Innovation at Imperial College London, 10 November 2015

'Cyber Essentials': Basic controls to mitigate the risk from common internet-based threats

The CESG's Cyber Essentials Scheme has been developed by Government and industry to provide a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet-based threats, within the context of the Government's 10 Steps to Cyber Security. It also offers a mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions. While we found evidence of the CESG's Cyber Essentials Scheme being implemented successfully within 20 health and social care organisations, it is not yet widely used in health and care.

ISO/IEC 27000 Series of standards: Internationally recognised comprehensive standard

The ISO/IEC: 27000 series of standards are recognised internationally as an effective and comprehensive standard. Most organisations using this standard seek accreditation of their implementations as a means of demonstrating to customers, stakeholders, regulators and others that information security has been independently assessed and validated. Whilst the properly implemented standard offers demonstrable benefits, the associated costs appear prohibitive for its adoption by many within the sector.

Practice (SoGP) were undoubtedly the most comprehensive and detailed available commercially, such standards were likely to prove to be overwhelming for those organisations lacking maturity in their cyber security capabilities. Once the cost of purchasing the licensed documentation and the necessary consultancy required for most organisations to successfully implement these standards are added to costs, the Review concluded that such standards were unsuitable and unaffordable for sector-wide implementation.

2.2.5 Conversely, the IG Toolkit, CESG's Cyber Essentials, and the 10 Steps to Cyber Security are available to use without expenditure on materials. They are deliberately focused upon organisations lacking mature cyber security capabilities, but which are willing to take steps towards creating and implementing controls to address the most prominent threats posed by network connectivity and internet-facing systems and services. By addressing these basic vulnerabilities, organisations can dramatically improve their ability to defend against basic threats, and to subsequently build upon this capability as part of a longer term improvement strategy.

2.3. New data security standards

2.3.1 **As illustrated above, the Review heard that data breaches are caused by people, processes and technology. Therefore it is upon these three themes that the Review has based its recommendations and standards.**

2.3.2 **The overarching message is that strong leadership is essential to all three themes.** The Review heard that a strong Senior Information Risk Owner (SIRO) makes a significant difference, and that Caldicott Guardians have had a positive impact where they have been properly supported. These established positions are viewed positively and can help to 'ensure organisational buy-in'[31]. However, there was some concern that other Board members would assume that security was something dealt with exclusively by the Caldicott Guardian or SIRO and therefore responsibility was not spread more widely, particularly in large organisations[32]. The board as a whole should take responsibility.

Recommendation 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.

31. Information Commissioner's Office, evidence session on security breaches, 6 November 2015
32. Interview with the Chief Executive and Deputy Director of Nursing, Royal College of Nursing, 25 November 2015

2.3.3 **Due to this need for strong leadership in data security, the Review has set out 10 data security standards clustered under three leadership obligations to address people, process and technology issues**:

- **Leadership Obligation 1:** People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.
- **Leadership Obligation 2:** Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.
- **Leadership Obligation 3:** Technology: Ensure technology is secure and up-to-date.

2.3.4 It is upon these obligations that the rest of this chapter is structured. It is important to note that the obligations and standards must apply to all organisations using health and care data, including commercial organisations. People are entitled to expect that their data will be protected wherever it is held.

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

Culture

2.4.1 **The Review heard that those who work within the health and social care system are motivated to provide the best possible quality of care to their service users and patients.** They want to deliver this care as quickly as possible using reliable information. When people are obliged to use technologies or processes that hinder or prevent them from doing their job, alternative solutions may be sought to help 'get the job done'[33]. Depending on individual judgement, this may result in data not being shared when it is safe and beneficial to do so or, conversely, shared when it is not safe to do so.

2.4.2 Staff behaviour was often cited as the unintentional cause of breaches, with 'simple errors, often compounded by heavy workloads, unclear or badly implemented policies and procedures. Mostly they can be described as naivety rather than deliberate non-compliance'[34]. The human element is considered one of the most relevant threat factors[35] and should be mitigated through tailored training for all staff.

2.4.3 However, there are some instances of negligence which are indicative of a failure to detect insecure behaviour or hold staff to account[36]. The Review heard that it was quite common for a letter to be sent to a wrong address, or a consultant to conduct a discussion with a patient in a busy ward where they can be overheard[37].

2.4.4 When considering what could help to address behavioural issues, consistent training, education and awareness emerged as being vital. As also found in Caldicott2, this was considered essential to addressing the culture of risk aversion, often resulting from a lack of confidence in security capability by senior management. Leaders should address cultural barriers by proactively engaging staff and involving national workforce organisations to support professional capability in this area.

2.4.5 Training alignment across health and social care organisations was suggested so that training in one organisation is recognised by another, to improve trust. The Review heard that the London Connect project has looked at a training passport for Information Governance, which would be transferable to other organisations[38].

2.4.6 As well as the proactive efforts made to train and educate staff, the Review heard from former members of the aviation sector about the importance of encouraging staff to speak up, and of listening to staff to derive valuable business intelligence to enable a swift reaction to a potential threat[39]. The Review heard that near misses, hazards and insecure behaviours must all be reported without fear of recrimination, and people should be encouraged to provide this valuable intelligence. In the airline industry, spikes in incidents are seen as people follow the good example set by staff speaking up about a threat, near miss or incident[40]. Unfortunately, in health and social care, increased reporting has been perceived as an indication of systemic issues and may prompt questions around what is wrong and who is to blame[41].

33. Provider Evidence Session, 27 November 2015
34. Information Commissioner's Office, evidence session on security breaches, 6 November 2015
35. Interview with Honorary Secretary, Royal College of GPs Evidence, 19 November 2015
36. Information Commissioner's Office, evidence session on security breaches, 6 November 2015
37. Expert Provider Evidence Session, 9 December 2015
38. Social Care Evidence Session, 24 November 2015
39. Chair of the Technology Assurance Committee, MONITOR, interview with Non-Executive Directors, 9 December 2015 and Interview with Head of ICT Operations, Imperial College Healthcare NHS Trust, 18 November 2015
40. Chair of the Technology Assurance Committee, MONITOR, interview with Non-Executive Directors, 9 December 2015 and Interview with Head of ICT Operations, Imperial College Healthcare NHS Trust, 18 November 2015
41. Commercial Provider Evidence Session, 18 November 2015

CASE STUDY 1: Bank of England – Helping staff to spot and report threats

The Bank of England provided the Review with an example of a simple way to help staff to spot and report threats before they turn into incidents. Phishing involves an email that appears to be from an individual or business that you know, but is from criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your computer. At the Bank of England, if a member of staff thinks they have had a phishing email, there is a custom button on Outlook for reporting it. Whether or not they open up an email and click on a link/attachment, users can press the button if they think it looked suspicious.

Data sharing: demonstrating trust

2.4.7 **The Review also heard of cultural issues concerning a lack of understanding of security and awareness, causing people to default to risk avoidance and an unwillingness to share[42].** Organisations and professionals stressed the need to ensure that the recipients of data have effective security in place. This is considered essential to integration[43]. It was recognised that data must be made available, but it was often felt that the potential recipients of data cannot be trusted due to poor or unknown security practices[44].

2.4.8 To facilitate data sharing, the Review proposes that the current IG Toolkit be redesigned and enhanced to become a portal for training material, guidance materials, exemplar documentation and Cyber Essentials support for all organisations, across health and social care should be provided.

2.4.9 A redesigned and enhanced IG Toolkit should become a central supporting tool to help embed the data security standards. The new toolkit should be enhanced to focus more on the common problems which all organisations face from a digital environment. It should enable organisations to learn from examples of good practice and measure themselves against a common set of criteria. The new toolkit must also be fully integrated with CareCERT and CERT-UK's Cyber Security Information Sharing Partnership (CiSP), both of which provide a platform for alerting the community to near misses and publicly known vulnerabilities in software packages. The new toolkit should also provide a mechanism through which to cascade lessons learned and intelligence gained from incident reporting.

2.4.10 An important requirement of the new toolkit would be to generate the business intelligence needed to measure capability across the sector – identifying the strongest and those most in need of support. Such business intelligence would allow the HSCIC to deploy more support to organisations most in need, and identify exemplar organisations that could help to support others in peer-to-peer partnering arrangements.

Recommendation 2: A redesigned IG Toolkit should embed the new standards, identify exemplar organisations to enable peer support and cascade lessons learned. Leaders should use the Toolkit to engage staff and build professional capability, with support from national workforce organisations and professional bodies.

2.4.11 **The first leadership obligation and the three data security standards supporting it are designed to ensure staff are equipped through training and standards, to be able to handle personal confidential data confidently**. Leaders must take data security seriously and support their staff in reaching these levels of competence.

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 only shared for 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 revised Information Governance Toolkit.

42. Executive Chair of Genomics England, interview 2 December 2015
43. Information Commissioner's Office evidence session on security breaches, 6 November 2015
44. Executive Chair of Genomics England, interview 2 December 2015

2.5. Processes: Proactively preventing data security breaches

2.5.1 'Processes' refer to the approved procedures which users are instructed to follow when performing business functions – either using technology, paper-based information, or a combination of the two. **The Review heard that when processes are poorly designed or communicated, users will often revert to doing something in the most convenient way**[45]**.**

2.5.2 **The Review heard the suggestion that security needs to serve as an enabler, so as not to be perceived as a blocker**. For example, the Review heard that in the NHS clinicians perceive that security is an obstacle to introducing innovation and digital health care and that the present standards do not reflect the obligations of the health workforce[46].

2.5.3 Processes should effectively support the needs of staff, otherwise unsupported alternatives may be sought in efforts to 'get the job done,' which could lead to breaches[47]. Throughout analysis of the evidence, a clear tension emerged between attempts to follow the security processes, and the practicalities of needing to access information. The Review heard that multiple logins take time, despite use of a smartcard, and access cuts out after a short period of inactivity[48].

2.5.4 To further reinforce the need for proportionality, simplicity and clarity, the Review heard strongly that 'IT security need to walk in the shoes of a clinician for a day'[49] and poignant statements such as 'the system that is supposed to support staff, doesn't'[50].

2.5.5 The Review heard of various tools and initiatives designed to help organisations maintain important processes. A key example is the efficient management of processes for 'joiners, movers and leavers'. This ensures that access to systems, data and premises is promptly granted and revoked, supporting the changing needs of the organisation and its employees. In some cases this may be hindered by ineffective communication with system administrators, whose role is to ensure that users' access to data is restricted to the requirements of their role. The Review received a case study showing how a simple analysis tool can identify risks such as unnecessary user or 'guest' accounts and the use of weak or default passwords. This provides a good example of the use of enabling technology to ensure that people follow the right process, supported by systems designed to identify and prevent inappropriate use. Transparent security measures such as these can assist in building and maintaining the public trust.

Recommendation 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 be also used by the IT companies that provide IT systems to GPs and social care providers.

2.5.6 Further examples were raised with the Review of areas where technology can remove significant risks associated with burdensome processes. Restricting the use of workplace technology for personal use of social media was supported, unless technology that will mitigate the risks is in place[51]. Likewise, the use of technology solutions to block all but the most sophisticated forms of email phishing attacks was raised as very effective[52]. More generally, it was suggested that it has been helpful for smaller organisations to be guided towards 'assured' cloud solutions, which are approved for use by some Government departments[53].

2.5.7 **The second leadership obligation, and the four data security standards supporting it, are therefore designed to ensure that those in leadership positions take responsibility for proactively preventing data security breaches and for responding appropriately to incidents or near misses, by making sure that processes support data security**.

CASE STUDY 2: The Palantir Dashboard – vulnerability analysis tool

The Palantir dashboard tool applies numeric risk values to users or groups of users and answers simple questions such as: 'How many unused accounts are there?' and 'How many accounts still have a default password?' The tool identifies irregular patterns of activity quickly and easily. This enables organisations to address simple but important issues quickly, or what could be described as 'low hanging fruit' for would-be cyber attackers. The tool supports the rule of thumb that 80% of cyber vulnerabilities can be addressed with 20% of your efforts.

45. Providers Evidence Session, 27 November 2015
46. Interview with the Director of the Institute of Global Health Innovation at Imperial College London, 10 November 2015
47. Interview with Chief Executive of NHS Improvement, interview, 18 November 2015
48. Interview with the Chairman of the Medical Ethics Committee & colleagues, British Medical Association, 23 November 2015
49. Expert Provider Evidence Session, 9 December 2015
50. Expert Provider Evidence Session, 9 December 2015
51. Interview with Head of ICT Operations, Imperial College Healthcare NHS Trust, 18th November 2015 – the example was provided of playing YouTube videos through sandboxing facility and separated from the corporate network.
52. Validation session with GCHQ experts, 17 December 2015
53. Validation session with GCHQ experts, 17 December 2015

CASE STUDY 3: Outsourced cloud services

Since the development of the Government Digital Marketplace and CESG's Cloud Security Principles, there are many approved providers of cloud services available to Government departments and agencies. Organisations can now outsource the secure management of IT infrastructure to certified expert companies, which operate at scale and rely on having a reputation for providing good security. Cloud services are effectively used in Government by the Cabinet Office, but use is relatively low in health and social care.

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 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 processes 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 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.

2.6. Technology: Secure and up-to-date technology

2.6.1 **Technology can be a key enabler when it proves to be effective in supporting staff to work simply and safely. The Review heard that in contrast, technology can become a source of risk when it is out of date and unsupported[54].**

2.6.2 The Review heard that some local IT systems in the health and social care sector are ageing and unsupported. These systems were not designed to feature modern security controls or to cope with large volumes of data and multiple users. When organisations attempt to implement security controls in outdated technologies, the resulting procedures can be counter-intuitive, inconvenient and easy to get wrong – or even ignored altogether. The Review heard that, to 'get the job done', users may seek convenient but less secure alternatives[55].

2.6.3 **There is significant use of software within the sector that is no longer supported by the manufacturer. This means that security fixes are no longer produced, leaving systems exposed to common types of cyber-attack.**

Cyber security

2.6.4 While the Review heard that outdated technologies are perhaps one of the most pressing issues facing IT infrastructure within the health and social care system, they are by no means the sole vulnerability. Technology must be properly configured to realise its potential and to afford the best protections possible. The extent to which health and social care organisations are leveraging security solutions to best effect is known to vary. The Review concludes that the organisations facing most risk are those with lower existing capabilities. Therefore the starting point in addressing cyber security must be simplified as far as possible to encourage full understanding, and be achievable within already stretched budgets.

54. HSCIC Evidence, November 2015
55. Providers Evidence session, 27 November 2015

2.6.5 The CESG's '10 Steps to Cyber Security' seeks to highlight the main areas of vulnerability for any organisation wishing to tackle cyber security in earnest. To support implementation of the 10 Steps to Cyber Security, the Cyber Essentials Scheme was launched as a means of standardising the implementation of affordable protections to the IT infrastructure, to help protect from basic cyber-attacks originating from the Internet. A standardised approach to implementing such protections enables compliance checking, comparison or benchmarking, and accreditation or certification designed for small businesses.

2.6.6 Use of the Cyber Essentials Scheme within the health and social care sector is limited to date, however, the Review found evidence of approximately 20 organisations using Cyber Essentials[56]. The Review recommends further testing of the Cyber Essentials scheme to evaluate its applicability and scalability within the health and social care sector.

Recommendation 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.

2.6.7 **The final leadership obligation and the three data security standards underpinning it are therefore focused on ensuring that secure and up-to-date technology is in place, both through the procurement process and the lifecycle of the technology within the organisation.**

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 which is 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 meeting the National Data Guardian's Data Security Standard.

CASE STUDY 4: Cyber Essentials successfully implemented at West Midlands Ambulance Service NHS Foundation Trust

West Midlands Ambulance Service NHS Trust previously held the ISO27001 accreditation. However, due to the associated resource requirements following an organisational restructure, a business decision was taken not to retain it. In obtaining Cyber Essentials the trust is able to provide its staff, the Board, business partners and service users with assurance regarding its overall cyber security posture, whilst maintaining resources and organisational focus upon its core clinical services and service users. In the Trust's opinion Cyber Essentials allows a more practical and pragmatic approach to cyber accreditation which meets the needs of flexible organisations whilst still addressing core security requirements. It also encourages buy-in from both technical and non-technical staff and stakeholder groups, thereby increasing general security awareness within the organisation.

'We view the Cyber Essentials accreditation as an essential technical companion to the NHS Information Governance Toolkit, which focuses upon less technical aspects of wider information security. We are aiming to use the accreditation as a foundation upon which to further enhance our security controls, thereby ensuring the ongoing confidentiality, integrity and availability of our systems and confidential data...'

Charles Knight, Head of Audit and Assurance Services & Gary Colman, Head of IT Audit an Assurance Services, West Midlands Ambulance Service NHS Foundation Trust

56. Information kindly provided by IASME (information assurance for small and medium sized enterprises) on 4 January 2016

2.7. Embedding the standards

2.7.1 **To be embedded fully and consistently, the data security standards must be mandated via mechanisms such as contracts**. The General Medical Services Contracts and NHS Standard Contracts are the mechanisms by which central government funds General Practitioners and NHS organisations respectively. This Review proposes that a provision requiring adherence to the new data security standards is written into contracts to make this a condition of full funding.

Recommendation 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.

2.7.2 **The Review recommends that organisations should provide objective, third party assurance of their compliance with the standards, for example as part of their internal audit mechanisms, and should build this into their routine mechanisms for reporting to senior management**. Objective assurance should be part of regular business procedures. For those organisations that are required to prepare statutory accounts, this should be delivered by a combination of the internal and external audit processes. For other organisations that are not required to prepare statutory accounts, this assurance may be delivered by some mechanism of peer review or interaction with HSCIC, for example through CareCERT, as agreed with the Department of Health and the relevant regulators.

Recommendation 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.

2.7.3 The Review recommends that data security should be integrated into inspection. **The Review recommends that CQC should integrate measures for compliance with the data security standards into their 'Well-Led Inspections' regime**. The Review anticipates that there will be a strong and natural link between the objective assurance that an organisation provides in respect of their compliance with the data security standards and the 'Well-Led Inspections' regime.

Recommendation 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 IG Toolkit to inform CQC of 'at risk' organisations, and CQC should use this information to prioritise action.

2.7.4 The Review heard from the primary care community in particular that they would value support to achieve the standards through a refreshed IG toolkit and expertise from the HSCIC. HSCIC could use the new toolkit to identify organisations that would benefit from additional support as well as exemplary organisations, and to put organisations in touch with each other for peer support. HSCIC should work with regulators to ensure that there is coherent oversight of data security across the health and care system.

2.7.5 Effective ongoing support from regulators and those supporting ongoing improvements in care is also essential. In July 2015, the Secretary of State for Health announced the formation of NHS Improvement to drive and support both urgent improvements at the frontline and the long term sustainability of the healthcare system. In social care, the Association of Directors of Adult Social Services in England (ADASS) furthers the interests of people in need of social care by promoting high standards of social care services and influencing the development of social care legislation and policy.

2.7.6 The Review heard of the need to foster a culture of 'learning not blaming'[57] where staff at all levels should be encouraged to highlight insecure behaviours, and alert management to their breaches or near misses. The evidence suggests that such knowledge constitutes powerful business intelligence[58], allowing organisations to target their security efforts at

57. Provider Evidence Session, 27 November 2015
58. Expert Provider Evidence Session, 9 December 2015

those people, processes or technologies which present the greatest risk to their information.

Recommendation 8: HSCIC should work with the primary care community to ensure that the redesigned IG 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 care system.

2.7.7 **Harsher sanctions should be put in place where there are malicious or intentional data security breaches.** This would ensure that there were clear consequences for deliberate security breaches, and give the public confidence that action can be taken where necessary to protect their information.

Recommendation 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.

2.7.8 The Review also believes it is important that there are more severe consequences when an organisation consistently fails to remedy a situation which, if left unresolved, may lead to a data security breach or data loss. This would include instances where a breach was not remediated in a timely manner.

The National Data Guardian's data security standards

These standards are intended to apply to every organisation handling health and social care information, although the way that they apply will vary according to the type and size of organisation. For example, GPs may want support from their system suppliers to identify and respond to cyber alerts in the first instance, and many social care organisations will want that from their Local Authority. Commissioners should take account of the standards when commissioning services.

Leaders of all health and social care organisations should commit to the following data security standards. They should demonstrate this through audit or objective assurance, and ensure that audit enables inspection by the relevant regulator.

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 only shared for 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 revised 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 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 processes 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 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 which is 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 meeting the National Data Guardian's Data Security Standards.

3. Consent/opt-out of information sharing in health and social care

3.1. Summary of evidence and analysis

3.1.1 **The evidence from the Review emphasised the importance of trust, clarity and purpose. The Review heard that trust is essential and should underpin any opt-out model**. '*Most people do not feel the need to know what is happening with their data, and people want to be able to trust the system and know that everything is okay*'[59]. Public views have not changed much since the 2013 Information Governance Review. There is still limited public knowledge about how data is used in health and social care. The NHS is trusted to collect, store and safeguard data and people expect information to be used for direct care. Some people are concerned primarily with privacy and the Review heard that data should be anonymised wherever possible[60]. Where data is anonymised, people tended to be much more comfortable with it being shared.

3.1.2 **Both patients and professionals emphasised the need for clarity and clear communications on when and what information professionals can and should share.** The Review heard that '*there is a lack of clarity on the current rights of individuals in relation to their data and the responsibilities of organisations [and individuals] in processing data*[61]. The Review also heard from GPs in particular that they would welcome clear guidance on their role as data controllers of their patients' GP records. National and local communications were cited as important both to educate the public about their rights and also to provide clarity to professionals about the legal framework and how they should act within the boundaries of the law[62].

3.1.3 The Review heard that people's opinions on their personal confidential data being shared for reasons beyond their direct care were influenced by the purpose for which it would be used; for example, there was concern about personal confidential data being used for insurance or marketing purposes. The Review tested different models, and concluded that **the opt-out model should be based on purposes that are communicated simply so that people can make an informed choice**.

3.1.4 In general, people were content with their personal confidential data being used for the care they received. However, people hold contrasting views about information being used for purposes beyond direct care and some people become concerned when data is shared outside the NHS 'family'. The Review heard convincing evidence on the need for information sharing between health and social care to facilitate integration of direct care and commissioning, and evidence about how different integrated care projects were meeting the challenge. The public sector, and specifically the NHS, is seen as more trustworthy than profit-making organisations[63]. In evidence sessions, individuals stated that people would need to be assured that 'the *government is able to safeguard and regulate the use of data in private companies if there is not an opt-out for this*'[64]. However, there is little awareness that private companies carry out NHS work or how those working for the NHS may carry out private work. For example, a hospital may contract with a private provider for direct care, health records are held by commercial IT system suppliers on behalf of providers, and Commissioning Support Units (which support CCGs to plan services) may be commercial organisations. The Review did not have the opportunity to explore this in depth with focus group participants. The Review took the view that the model should be set around the purpose to which data is put and its potential benefit to patients and service users, and that dividing up NHS and 'non-NHS organisations' without reference to purpose can be artificial and misleading.

3.1.5 The differing opinions presented to the Review from both professionals and the public demonstrates that there is no easy answer to opt-outs that will please everyone.

59. Interview with representative from national patient representative charity National Voices 1 December 2015
60. Testing sessions showed different interpretations of what is meant by anonymised data. For example some members of the public referred to removing a name whereas others suggested an understanding of protections e.g. 'classifying the data differently'.
61. Patients, service users and carers evidence session, 24 November 2015
62. Research evidence session 18 November 2015, RCGP 19 November 2015, ICO evidence session 6 November 2015
63. Focus groups and Stevenson, F., Lloyd, N., Harrington, L., Wallace, P., (2013) Use of electronic patient records for research: views of patients and staff in general practice. Family Practice Vol 30 (2) pp. 227-232
64. Interview with representative from national campaign group 23 November 2015

3.2. Developing an opt-out model

3.2.1 **The Secretary of State for Health asked the National Data Guardian to develop a consent/ opt-out model which makes it absolutely clear to patients/users of care when health and social care information about them will be used and in what circumstances they can opt out.**

3.2.2 The Review considered whether patients and service users should be able to opt out of their personal confidential data being used for purposes beyond care or whether they should be asked for their consent to opt in. Some evidence indicates that people would like to be asked, but our focus groups found that participants were generally supportive of data being used to run the health and social care system and for research. During testing people categorised as 'well' were generally less in the know and some admitted they had '*never really thought about it all*'. Others *'didn't care about their data being used'*[65]. Whilst many people may not actively engage in the use of their data they do expect medications to be safe, threats to public health such as Ebola to be monitored, and to have appropriate local services available to them. These rely on high quality data, which covers a significant proportion of the population. The Review was persuaded that the best balance between meeting these expectations and providing a choice to those who have concerns is achieved by providing an opt-out model. **The review concluded that people should be made aware of the use of their data and the benefits; an opt-out model allows data to be used whilst allowing those who have concerns to opt out.**

The need for information

3.2.3 **Information is essential for high quality health and social care – to support the running of the health and social care system; to improve the safety and quality of care, including through research; to protect public health; and to support innovation. Data sharing is essential to identifying poor care. It is clear that more effective data sharing could have enabled some of the recent failures to provide proper care to patients to be identified and tackled earlier**. It can also be beneficial to join health data up with other types of information, to provide better services to people. The way that information is shared across the health and social care system to support its management is complex and has evolved over time. There are multiple systems and organisations involved in processing data for a range of purposes. This means that explaining benefits can be lost in the complexity.

3.2.4 During the Review some people expressed the view that receiving NHS care was a type of 'social contract' and patients should not be able to opt out of their information being used for direct care or for running the NHS[66]. In return the system should protect data and if the trust is broken, through a breach, repercussions should be expected. However, the Review found that many people did not hold this view. In some instances this was because they held strong concerns about who might see the information and what might be done with it. Some argued that this could be countered by more being done to explain the benefits of data sharing. The recently published report from the House of Commons Science and Technology committee also recognises the importance of explaining the benefits of data sharing to individuals and society and giving citizens greater control over how their data is used.

Recommendation 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.

Direct care purposes

3.2.5 **There continues to be a low level of public awareness and understanding of how health and social care information is used, but an expectation that information is shared for direct care[67].** Since the last review, new legislation has been introduced which places a legal duty on health and adult social care organisations to share information when it will facilitate care for an individual[68]. This reinforces Caldicott principle seven, which sets out that 'the duty to share information can be as important as the duty to protect patient confidentiality'. The Review heard examples where information was not being shared for direct care. A patient dying of lung cancer was visited by his GP, community nurse and hospice nurse in one day each asking the same questions, because information was kept separately and not shared within the team caring for the patient. The patient's wife subsequently complained about the lack of communication between those caring for her husband at a very stressful time.

65. Evidence from public focus groups
66. Representatives NHS England; Public Health England; and some GPs involved in commissioning expressed views around this e.g. particularly where commissioners are working closely with providers of care
67. The Review's patient focus groups found that beyond an understanding of patient records being used to help deliver care, knowledge about how data is collected and used was extremely limited. This was also found by Ipsos MORI. Ipsos MORI (2007) The Use of Personal Health Information in Medical Research General Public Consultation. Medical Research Council. Ipsos MORI, (2014) Public attitudes to the use and sharing of their data. Royal Statistical Society.
68. The Health and Social Care (Safety and Quality) Act 2015, which inserted sections 251A, B and C into the Health and Social Care Act 2012: (http://www.legislation.gov.uk/ukpga/2015/28/contents/enacted)

3.2.6 The Review heard that patients may have elements of their record that they do not want to be shared and felt that sharing their whole record was not necessary for direct care[69]. **In line with the Caldicott principles and the last review, only relevant information about a patient should be shared between health professionals in support of their care.** Explicit consent should be obtained before accessing someone's whole record.

3.2.7 In focus groups of members of the public, the Review heard that people were comfortable with data being shared with care professionals for their care, but not anywhere else within the local authority. There was a concern that social care departments might share data with the rest of the council e.g. housing or finance[70]. The Review also heard that people may be surprised that information was shared across health and social care: '*If a social worker say wants to access your medical records, I think you should sign a form giving your consent'*. The Review heard that in social care it is common for people to be asked explicitly about what information may be shared, and with whom – for example, in Hampshire County Council social care users are asked for their explicit consent about how their personal confidential information can be used.

3.2.8 Changes in the delivery of care and information sharing, driven by the Five Year Forward View[71] and local imperatives, are breaking down traditional divides between primary care, hospitals, community, mental health and social care services. Services are increasingly being planned across organisational boundaries and extended teams may be involved in providing care to an individual including from voluntary sector organisations. In some instances this requires a step change in the relationship and trust between different health and social care commissioners, providers and professionals*: 'Social care providers can be seen as outsiders and not trusted with data*'. In particular, the Review heard that there are still barriers to information being shared with un-regulated social care staff: *'People are afraid to share at the moment because there's no reassurance that other professions meet the same standards'*[72]. However, there is increasing recognition that these behaviours are unhelpful and outdated: *'If a future health and social care service is based on integrated care, it will rely on data sharing'*[73].

3.2.9 It is important that the public are made aware of these changes, and as set out in the last Review, **there should be 'no surprises' for the individual about who has had access to information about them**. All organisations processing information, e.g. providers, CCGs and Local Authorities, should ensure that fair processing information is available. It is also important that information is shared where appropriate to support care. In areas pioneering integrated care and new models of care, the Review found evidence of successful approaches to meeting people's expectations and making sure that professionals had the information they need. The Review recognises the need to make appropriate data sharing easier in order to support integrated health and social care.

3.2.10 The Review considered risk stratification for case finding which involves health professionals identifying individuals who may benefit from targeted inventions. Personal confidential data is needed so that the health professional, e.g. the GP, can offer an individual preventative care; this would be part of direct care. Patients would expect that health

CASE STUDY 5: Leeds Care Record

Patients in Leeds are benefiting from healthcare professionals directly involved in their care having access to their relevant health information. By logging on to the Leeds care record and simply clicking on the relevant organisational tab, healthcare professionals can see the latest information about their patient. Information from GP practices, hospitals and mental health is live on the record and a pilot of community services is under way, with social care to follow.

Those working in hospital clicked on the GP 'tab' 4,000 times in a month, which could represent a significant saving in terms of time that would otherwise have been spent phoning the GP practice. Local engagement has taken place with professionals and patients to define the data which is made available on the care record. Patients have been informed about the Leeds care record using a variety of techniques including leaflets and posters in GP practices, media coverage and local engagement events. The care record has been operational for more than 18 months and so far 67 out of 760,000 patients in Leeds have chosen to opt out.

69. In the public Policy Lab workshop the Review heard: 'If I was a drug user I wouldn't want a community nurse who was coming to treat my ulcers to look down on me for being a drug user. You would have to make it clear who will see this and who will not.' At the Patients, Users, Carers Evidence Session, 24 November 2015 and Policy Lab workshop 10 December 2015 individuals also stated that patients would expect to be able to opt out of information being shared for direct care, as they can now.
70. Social care evidence session 24 November 2015
71. https://www.england.nhs.uk/wp-content/uploads/2014/10/5yfv-web.pdf
72. Caldicott2 highlighted good practice around appropriate sharing of personal confidential data between registered professionals and non-regulated staff
73. Interview with NHS England 18 November 2015.

CASE STUDY 6: Whole System Integrated Care Record (WSIC)

Patients in London are more likely to have their information available at the point of care following developments across the capital. A Whole System Integrated Care (WSIC) record is enabling information sharing between health and social professionals in North West London. One of the aims is for the health and the social care systems to work together to improve care services.

Communication materials are provided for GPs and social care professionals to support communication with the public. Patients and service users are informed that their care information may be shared with acute services consultants, mental health consultants, community health professionals and social care workers directly involved in their care.

Patients can opt out of their information being made available outside a particular care setting. In addition, the North West London care information exchange will provide patient and service users with a single view of their information with the ability to control information sharing.

In both these examples, an integrated record is created on the basis of implied consent. Smart cards and role based access controls ensure that only information relevant to a job role is viewed and information sharing agreements are in place. Explicit consent is obtained before a patient's Whole System Integrated Care Record is accessed.

professionals would use data they hold to improve their care on the basis they could dissent from the treatment when offered. However, some CCGs are using the same predictive tool for both risk stratification for case finding and risk stratification for planning. The Review suggests that these two functions are separated. The Review considers that risk stratification for case finding, where carried out by a provider involved in an individual's care or by a data processor acting under contract with such a provider, should be treated as direct care for the purpose of the opt out (and therefore should not be subject to the opt out of personal confidential data being used for purposes beyond direct care.)

3.2.11 There are some elements of direct care which rely on the processing of data nationally, for example the electronic transfer of prescriptions, screening[74], immunisation programmes and the Summary Care Record. **The Review heard no evidence to suggest that there should be a change to effective local or national arrangements for sharing information.** However, multiple opt-out forms are confusing for patients and health and social care professionals. In West Hampshire, a number of GP practices are working collaboratively to provide same-day appointments to patients. A GP described how a patient would attend from a different practice, but their record cannot be accessed because they have opted out of their information being shared. Often the patient response is '*I didn't mean that, please can you opt me in again?'* However, this is not possible unless they return to their registered practice. As well as being confusing, opt-out forms do not reflect the granularity of people's concern, as individuals may worry about a very specific piece of information. The Department of Health, working with other stakeholders, should consider how this is addressed.

3.2.12 The different successful approaches being taken at local level led the Review to conclude that an overarching, national, consent question should not be framed around direct care. **A person can still ask for their health care professional not to share a particular piece of information with others involved in providing their care[75].** This may be in relation to a local shared record programme. Local communication materials should inform people what they should do if they have concerns.

Purposes beyond direct care

3.2.13 The Review considered the extent to which personal confidential data was needed for purposes beyond direct care. **The Review heard that high quality, linked data was required for running the health and social care system and improving the safety and quality of care, but that for the majority of purposes personal confidential data was not required.**

3.2.14 The purposes where personal confidential data are needed are as follows:

(i) **Commissioning** – NHS England, commissioners in CCGs and Local Authorities play a valuable role

74. Caldicott2 provides further information about screening

75. If withholding information would result in a patient receiving unsafe care, it should be explained to the patient that it will not be possible to arrange effective treatment for them without disclosing information (GMC guidance)

in improving the care of patients. The Review heard examples of local commissioners working closely with health and social care professionals to coordinate care and evaluate the impact of new services or interventions resulting in improvement to the care patients receive. Evidence received from NHS England, which was informed by feedback from local commissioners, set out the specific circumstances when commissioners require personal confidential data:

- invoice validation of non-contracted activity;
- national patient surveys;
- analyses where the level of geographical precision required necessitates the use of personal confidential data e.g. to consider the impact on its patients of a GP practice moving premises;
- ensuring that cohorts of patients with highly individual needs are treated in the most appropriate setting, e.g. detecting patterns in relation to the care of patients with learning disabilities.

Concern was expressed about the impact of an opt-out on the quality of data for these purposes – for example, resources may be allocated on the basis of incomplete information, or unusual trends which may indicate unsafe care might not be highlighted[76]. The Review considered whether to exclude from the opt-out the use of data for purposes which enable direct care such as planning local services. However, the use of information for this type of purpose was 'new news'[77] to the public and there was a lack of knowledge and interest in this type of data use. Public engagement suggests that understanding of direct care did not align with an extended definition at the present time. The Review is keenly aware that public attitudes are likely to change as more information about the potential benefits of increased data usage are provided.

(ii) **Monitoring health and social care services** – CQC is a statutory body, which is responsible for monitoring, inspecting and regulating services to support the improvement of care. Personal confidential data is used as part of its NHS outliers programme. Statistical methods are used to identify unexpected performance (outliers) in mortality or maternity indicators that may be linked to problems with the quality of care. Part of this process can include alerting the provider, using the NHS number, to the individual patients. In addition, CQC monitors the care of people moving between adult social care residential services and hospitals so that action can be taken to protect people using services. The CQC also coordinates the NHS Patient Survey Programme, which allows patients and the public to have a say about the quality of NHS services[78].

NHS Improvement is responsible for supporting urgent operational improvements and ensuring long-term sustainability of the healthcare system[79]. Personal confidential data is required to audit the quality of hospital data[80] by comparing it to patient records.

Clinical audits are used to check whether healthcare is being provided in line with agreed and reputable standards e.g. those of NICE[81]. Regulators, those providing care, and the public can see what is working well and where improvements can be made. The use of personal confidential data for local clinical audit is permissible within an organisation with the participation of a health and social care professional with a legitimate relationship to the patient through implied consent[82]. For audit across organisations, the use of personal confidential data is permissible where there is approval under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002. NHS England commissions the Healthcare Quality Improvement partnership (HQIP) to manage 30 national audits[83] and there are also 20 clinical audits, which are funded by the specialist societies themselves.

(iii) **Public health purposes** – Protecting and improving the nation's health and wellbeing and reducing health inequalities are fundamental to the health and social care system. As set out in the 2013 review, some uses of information for public health purposes can be seen as direct care, i.e. where they relate to the care of an individual. This includes the oversight and provision of population screening programmes[84]. There is an overriding public interest for using personal confidential data for some public health functions, e.g. the control of outbreaks of infectious diseases. These are discussed in further detail below.

(iv) **Research** – Research is an essential part of improving the safety and quality of care: research facilitates the development of innovative new medicines, treatments and services. The National Research Ethics Service provides an ethical review

76. Meetings with stakeholders including NHS England, NHS Improvement and CQC
77. Evidence from public focus groups
78. http://www.nhssurveys.org
79. It brings together Monitor, the NHS Trust Development Authority (TDA) and patient safety and improvement functions from across the NHS.
80. Hospital Episode Statistics (HES) and Secondary Uses Service (SUS) data
81. https://www.nice.org.uk
82. As set out in Calidott2
83. http://www.hqip.org.uk/national-programmes/a-z-of-nca/
84. Even though authorised under the Health Service (Control of Patient Information) Regulations 2002

CASE STUDY 7: Information sharing in Worcestershire and elsewhere

In Worcestershire, commissioners estimate that approximately 35% of their local budget is spent on 1% of their population. Commissioners are using this information to identify a cohort of people who will be provided with an individual care and support package. A separately allocated budget for this cohort will help incentivise those providing care across different organisations to work together to deliver better outcomes.

Analysis undertaken by Midlands & Lancashire Commissioning Support Unit (CSU) for commissioners uses person-level data drawn across health and social care. This data is linked through a unique identifier based on the NHS Number in the CSU to identify the cohort of people most in need of joined-up care and support.

The CCGs and the County Council, which is responsible for providing social care services, then need to track this cohort of patients to monitor the impact of interventions. For example does an investment in specialist nurses in the community reduce admissions to hospital? The CCG and County Council create a list of the cohort of patients, which is shared with those providing care. This allows the care provided and payments to be tracked and allocated to the separate budget.

of all health research involving patients in England. Researchers have worked hard to gain the trust of research participants: 2.2 million patients have agreed to take part in medical cohort studies, and the Review heard that this valuable contribution should not be undermined[85]. The Review also heard that there is support for information being used for research, but that 'the public is likely to react differently to research that does not have a link back to improving direct care'. Personal confidential data is currently used for research with explicit patient consent or where there is approval under the Health Service (Control of Patient Information) Regulations 2002. These Regulations can support research use where there is no practicable alternative to reliance upon them: where neither consent, nor the use of data that is not identifiable, can be practical alternatives. Decisions on approval are taken by the Secretary of State or the Health Research Authority with independent advice from the Confidentiality Advisory Group[86].

The consent/opt-out model

3.2.15 **The Review found that there is support for data being used for running the health and social care system and for improving the safety and quality of care when the benefits of doing so are clearly explained[87].** In public focus groups and in the Policy Lab testing workshop the Review heard that when individuals were given information explaining uses other than for direct care, such as planning services and research, these uses were regarded as beneficial and sensible: '*The data is there, so it should be used*'[88]. The Review also heard that people want a choice about how their personal confidential data is used and to understand the types of organisation that are accessing data. The public tended to make a distinction between the NHS 'family' and others making use of data[89].

3.2.16 The Review tested a model giving two opt-out questions with patients and health care professionals in response to hearing that some patients made a distinction between sharing within and beyond the NHS 'family'. In this testing the first opt-out related to personal confidential data being used for essential purposes to run the NHS, e.g. planning services and funding care; the second opt-out related to the monitoring and improving the quality of care through research. For each question, patients and healthcare professionals were given scenarios to support understanding of the two different choices. The Review was told by both the public and professionals that there was confusion about how the existing system worked, what the new opt-outs related to and how the two categories of information differed[90].

3.2.17 The Review then considered providing greater clarity and developed two opt-outs which stakeholders thought were clearer and gave a more helpful distinction. These two opt-outs were:

(i) providing local services and running the NHS and social care system. This would cover the use

85. http://www.mrc.ac.uk/publications/browse/maximising-the-value-of-uk-population-cohorts/
86. http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/
87. Existing literature on public opinion shows that when individuals are Existing literature on public opinion shows that when individuals are informed about data sharing and its benefits their support for the project increased, see GMC (2007). Public and professional attitudes to the privacy of healthcare data. A survey of the literature. http://www.gmc-uk.org/GMC_Privacy_Attitudes_Final_Report_with_Addendum.pdf_34090707.pdf
OPM (2015) Review of public and professional attitudes towards confidentially of healthcare data. http://www.gmc-uk.org/Review_of_Public_and_Professional_attitudes_towards_confidentiality_of_Healthcare_data.pdf_62449249.pdf
88. Public focus group.
89. The engagement events and analysis of existing literature on public opinion showed that people become concerned about data sharing when their data is accessed outside the NHS, especially with commercial organisations or those looking to profit from data usage. Stevenson, F., Lloyd, N., Harrington, L., Wallace, P., (2013) Use of electronic patient records for research: views of patient and staff in general practice. Family Practice Vol 30 (2) pp. 227-232
90. Public focus group and testing workshops with patients and health and social care professionals

of personal confidential data by registered providers, statutory bodies using data for their statutory purposes and the Royal Colleges undertaking national clinical audit. The relevant statutory bodies are NHS England, NHS Improvement, Public Health England, the Care Quality Commission, Clinical Commissioning Groups and Local Authorities. This would also include organisations which process information on behalf of statutory bodies for their statutory purposes, e.g. CSUs processing data on behalf of CCGs.

(ii) supporting research to improve treatment and care. This would cover the use of personal confidential data to support research and improve the quality of care. These applications are currently approved by the Secretary of State or the Health Research Authority with independent advice from the Confidentiality Advisory Group.

3.2.18 As an alternative, the Review also looked at a possible single opt-out for personal confidential data being used for purposes beyond direct care. This has the advantage of being a simple message for the public, and would be simpler to implement both locally and nationally. However, there was subsequent concern that a single opt-out would limit people's choice. The review heard from those running the system that it could result in people who are content for their information to be used for core health and social care uses, such as planning local services, opting out due to their concern about broader uses such as research.

3.2.19 Further testing was then conducted of both a two-question and a single question model. This showed that some people were fully supportive of data sharing and agreed with the need to find the right balance between using data for the benefit of patients and the wider NHS, and keeping that data safe. People were very interested in the language used to describe the choices, and one group recommended that the language should be as simple and direct as possible, with clear examples of the impact of either sharing or not sharing data.

3.2.20 A summary of the two models and indicative questions are set out at the end of this chapter. It was clear throughout the Review that public understanding of the current arrangements for data sharing is limited; when communicating choices, there is an assumption that the data flows are new and therefore controversial. The Review recommends that there should be a formal, full and comprehensive consultation on the proposed consent/opt-out model. Alongside that consultation, there should be further testing of both a two-question and a single question model with patients and professionals to see if people would prefer to have more than one choice. Following the consultation and testing, further work on the wording would be needed before the model is ready for implementation.

Recommendation 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.

3.2.21 **Whilst patients have a right under the NHS Constitution to request that their personal confidential data is not used beyond their direct care, there is currently no easy way for them to do that. The Review suggests that the new opt-out model should be implemented by every organisation which shares health and social care information.** Where someone has opted out this choice should be respected by data controllers (subject to the exceptions outlined in the exceptions and overrides section below). Ultimately, a patient should be able to state their preference once (online or in person) and be assured that this will be applied across the system. They should be able to change their minds if they wish, and this new preference should be honoured. This would be a significant step forward in allowing people to more easily state a preference about the use of their health and social care information.

3.2.22 **There is confusion amongst care professionals and patients about the law in relation to confidentiality**. For example, the requirements under the Data Protection Act 1998 and the Common Law duty of Confidentiality are often confused. The Review suggests that the ICO and Information Governance Alliance (IGA) should work jointly to make the relationship between the two clear for local practice including social care[91].

91. The ICO has recently consulted on a code of practice on communicating privacy information to individuals which is part of a range of guidance provided by the ICO to support organisations in meeting DPA requirements (https://ico.org.uk/about-the-ico/consultations/privacy-notices-transparency-and-control-a-code-of-practice-on-communicating-privacy-information-to-individuals/)

3.2.23 **The Review recommends that the new model should apply to uses of personal confidential data that are specifically authorised under law**, e.g. in accordance with Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002. Where a patient does *not* opt out this does not mean that they have consented for their information to be used for purposes beyond direct care. In the absence of consent, there will always need to be a specific legal authority for sharing (e.g. in accordance with regulations under section 251 of the NHS Act 2006). There will also be some specific circumstances where an individual's decision to opt out does not apply, as set out under 'exceptions and overrides' below.

3.2.24 This is consistent with the stance taken by the Confidentiality Advisory Group (CAG). CAG provides independent expert advice on whether applications to access patient confidential data without explicit consent should be supported under Regulations 2 and 5 of the Health Service (Control of Patient Information) regulations. It has taken a position that it will advise that it is not in the public interest to override an opt-out in anything other than the most exceptional circumstances, e.g. serious public safety concerns.

Use of anonymised data

3.2.25 **The majority of purposes beyond direct care do not require personal confidential data:** those commissioning, regulating, and monitoring services, or undertaking research, often do not need to know the identity of an individual. Instead they either require high quality linked person level data, which allows them to track patients without knowing who they are, for example to track patients with asthma who are repeatedly admitted to hospital, or aggregate/statistical data, for example to count how many patients in England have asthma.

3.2.26 The previous Review on Information Governance described two types of data: (i) de-identified data for limited access and (ii) anonymised data for publication. This was based on the definitions in the ICO's Anonymisation Code of Practice[92]. **The Review considered whether the opt-out should apply to de-identified and anonymised data. The Review heard that the public is broadly content for their anonymised information to be used for health and social care purposes**: '*I think if it's kept anonymous, then it's not a problem. If they share it, they wouldn't have your name against the data*'[93]. The definition of anonymised provided by the public was closer to de-identified for limited access, e.g. removing a name. The Review heard that the public was concerned about protections in place to safeguard their data.

3.2.27 **The Review also heard that de-identified data is of considerable benefit to commissioners, planners and researchers. They were concerned that an opt-out would have a negative impact.** For example, CCGs would not have a complete dataset for their population including patients with complex care needs, regulators would not have complete data to look at trends for example in relation to the quality of care[94], and researchers may not be able to answer questions confidently, such as how many people have a certain condition or to identify associations between causes and health effects[95].

3.2.28 De-identified data and anonymised data are widely used in the health and social care system. Data which does not identify individuals has been used to understand the future health needs of the population, for example to inform NICE cancer guidance and ensure the safety of drugs and medication. Also, the safety of the MMR vaccine was confirmed using de-identified data. A complete set of de-identified data enables NHS Improvement to conduct system level analysis of patterns, consider what is working well and where improvements are needed, develop payment tariffs, and improve the quality of data relating to the cost of care as part of its costing transformation programme.

3.2.29 **In future, more person-level data will be required by commissioners because services will increasingly be integrated around an individual, which means that commissioners will need to understand the impact of interventions on cohorts of patients and service users, as well as on organisations and the local population as a whole.** Since the last review, it has become evident that a significant amount of work has been undertaken to help support commissioners to have appropriate access to information[96], but commissioners stated in the Review that they were still experiencing challenges in relation to accessing the data required to carry out their statutory functions. The absence of data, particularly from GP practices and social care, makes it difficult for commissioners to evaluate the impact of interventions across all care settings[97]. One commissioning GP said: '*What would members of the public think if they knew the NHS could not fully account for the money it is spending? It should be a standard part of the business*'. A driver for using

92. https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/
93. Public focus groups
94. Evidence from CQC.
95. Evidence from Medical Research Council.
96. For example a draft document 'Enabling Information Sharing: A User's Map for Health and Social Care' sets out six reasons for sharing information informed by the experience of local integrated care pioneers and vanguards, systems.hscic.gov.uk/infogov/iga/consultations/nhsenframework.pdf
97. A recent National Audit Office report states: 'The Department and NHS England are taking steps to improve access but they are making decisions without fully understanding either the demand for services or the capacity of the current system. Given the important role general practice plays in the health and social care system, the Department and NHS England need better data in order to make well-informed decisions about how to use limited resources to best effect. (https://www.nao.org.uk/wp-content/uploads/2015/11/Stocktake-of-access-to-general-practice-in-England.pdf)

CASE STUDY 8: Use of linked data in East and North Hertfordshire

Health and social care services in East and North Hertfordshire are using MedeAnalytics' (http://medeanalytics.co.uk) software to better understand their local population. As East and North Hertfordshire emphasised, the tool's benefit is that it facilitates data-enabled decisions and valuable insights visible to users. Having access to timely, linked data about local patients and service users has enabled East and North Hertfordshire to undertake powerful impact analysis of their re-ablement service (helping people regain their independence) and set up automated information alerts – for example, advising a GP if one of their patients is making frequent visits to A&E.

Identifiers such as name, NHS number, and full postcode are coded rather than removed altogether. This means that where an individual is identified as being at risk or in need of a specific intervention, the relevant health and care professional involved in the care of the patient can use the system to re-identify the individual or individuals and make the necessary intervention.

personal confidential data has been the absence of high quality linked person level data[98]. This absence results in the NHS number and postcode being used to link data, check the quality of the linked data, and to track patients for example to monitor the impact of interventions or check the quality of care. The review found no reason for commissioners to access personal confidential data for risk stratification for planning if they were provided with de-identified linked data and the function was separated from risk stratification for case finding, as set out in the direct care purposes section above.

3.2.30 The third Caldicott principle calls for the minimum amount of personal confidential data to be transferred or accessible as is necessary for a given function to be carried out[99]. That is best achieved by encouraging organisations to switch from using personal confidential data to de-identified data for limited access or anonymised data. East and North Hertfordshire CCG has explored the benefits of using de-identified data.

3.2.31 The Review heard strong evidence from organisations such as NHSE, NHSI and CQC about the importance of high quality person level data for running the health and social care system, to protect public health and support research. Most purposes do not need personal confidential data, but do require a subset of information drawn from a full dataset. **The Review proposes that personal confidential data should be passed to the HSCIC, as the statutory safe haven of the health and social care system, to de-identify or anonymise and share it with those that need to use it.** If HSCIC were able to disseminate high quality anonymised data based on a complete dataset, it would reduce the need for these organisations to access personal confidential data. For that reason the Review recommends that, in due course, the opt-out should not apply to any flows of information into the HSCIC. This requires careful consideration with the primary care community, which take its responsibility as data controller seriously, and with the public. It would, however, enable commissioners, for example, to fulfil many duties currently subject to Confidentiality Advisory Group (CAG) recommendations, without requiring access to personal confidential data. For the time being the status quo should prevail. The Review notes the Government's decision to change the name of HSCIC to NHS Digital. This will provide the organisation with a good opportunity to use the NHS brand making it clear to everyone that it is part of the NHS 'family'.

Recommendation 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.

3.2.32 **The Review recommends that the good practice advice contained in the Information Commissioner's Office Anonymisation Code should be used to safeguard all de-identified data.** The Code provides advice on how to turn data into a form which 'does not identify individuals and where identification is not likely to take place'. The code sets out how any risk of re-identification can be mitigated where there is limited access for a specific purpose by the use of contracts and other controls. The ICO code covers various techniques that can be used to convert personal confidential data into de-identified data, to

98. Evidence from statutory bodies including NHS England and local CCGs.
99. Caldicott 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."

produce anonymised data but on a person-level basis. The code shows that the effective anonymisation of personal confidential data is possible and desirable and can help society to make use of rich data resources whilst protecting individuals' privacy.

3.2.33 The ICO has the powers to issue monetary penalty notices of up to £500,000 for serious breaches of the Data Protection Act. Under the EU General Data Protection Regulation (GDPR)[100], these sanctions will increase to a maximum of £20 million for public bodies and 4% of global turnover if a private company. The recently published report from the House of Commons Science and Technology committee[101] recommends that the Government introduces criminal penalties for serious data protection breaches. In response to the committee[102], the Government has pledged to review the existing sanctions regime, as the GDPR is implemented. **The Review welcomes this work and recommends that the Government should consider introducing stronger sanctions to protect anonymised data. This should include criminal penalties for deliberate and negligent re-identification of individuals.**

3.2.34 **The combination of recognised national guidance for anonymisation alongside severe penalties for serious breaches of the Data Protection Act 1998 enables the Review to propose that data that has been de-identified according to the ICO's Anonymisation Code should not be subject to the opt-out. The review recommends that the forthcoming Information Governance Alliance guidance on Anonymisation for health and social care, which is intended to support the ICO Code, should explicitly refer to the potential legal, financial, and reputational consequences of organisations failing to have regard to the ICO Code by re-identifying individuals.** The anonymisation guidance could also be used to underline the need for all those that use health and social care data, such as universities, to work with the same approach.

Recommendation 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.

Recommendation 14: The forthcoming Information Governance Alliance'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 Anonymisation Code of Practice by re-identifying individuals.

Contributing to a specific research project

3.2.35 **People should continue to be able to give their explicit consent separately if they wish, e.g. to be involved in research, as they do now.** They should be able to do so regardless of whether they have opted out of their data being used for purposes beyond direct care. This should apply to patients' decisions made both before and after the implementation of the new opt-out model. There are local and international examples of effective solutions.

3.2.36 There is also evidence of controlled environments, safe havens or research banks being successfully implemented on the basis of explicit consent where personal confidential data is required. There is scope for further innovation in this area.

CASE STUDY 9: UK Biobank

UK Biobank holds data and clinical samples to support longitudinal research on more than 500,000 people. It can initiate requests for participants to submit tissue samples and undergo diagnostic tests and can also link to data held by a participant's GP. The consent model is explicit and facilitated by an in depth consultation process.

UK Biobank makes use of a three part model to withdraw consent enabling participants to: withdraw consent to be contacted in future, but allowing the organisation to continue to draw information from a medical record and to use existing samples taken; withdraw consent for any future use of data, but retaining Biobank's ability to use samples and data collected previously; or to completely opt out of the system, where Biobank would delete a participant's data and destroy any remaining samples.

100. The Regulation is published in the Official Journal – http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
101. Science and Technology Committee Report http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/468/46802.htm
102. Government response to Science and Technology Committee Report http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/992/992.pdf

CASE STUDY 10: HealthBank (Switzerland)

HealthBank is a for-profit co-operative company, based in Switzerland. Individuals (members of the public) pay £65 to join as a shareholder and upload their own health data as they see fit. Shareholders are asked explicitly to contribute their data to research trials and are paid for their efforts (and data) at a price stipulated by the study owner. In this way, HealthBank offers an 'opt-in' model whereby shareholders choose, on a study by study basis to donate or sell their data. As explicit informed consent is required, no specific legal gateway is required for the sharing of confidential data.

Recommendation 15: People should continue to be able to give their explicit consent, for example to be involved in research.

Genomics

3.2.37 Genomics offers huge potential for personalised medicine to improve the effectiveness of healthcare while reducing or eliminating side-effects. However, the lines between direct care and secondary use of data are blurred: interpreting the clinical significance of an individual's genomic variants is reliant on the data of larger cohort of patients with similar disorders. The timescales of the Review have not enabled a detailed consideration of this area. Useful work has taken place on these issues, for example a recent joint report from the Public Health Genomics Foundation and the Association for Clinical Genetic Science makes a number of commendable recommendations[103].

3.2.38 The 2013 Information Governance Review considered the issue of consent for consent, where researchers may need to access personal confidential data to identify people with particular characteristics to invite them to take part in clinical trials and other interventional studies; this is considered as good practice. This Review has not received any evidence that the professional standard and good practice in relation to consent for consent, as set out in the last report, needs to be re-examined.

National disease registers

3.2.39 Public Health England (PHE) maintains national registers of diseases including cancer, congenital anomalies and rare diseases. These registers have played a vital role in improving outcomes for many patients. The Review heard evidence that such registers rely on completeness of data and linkage for their validity. The Review understands that PHE intends to enhance the level of consent taking for its disease registers, by contacting patients directly where appropriate at the point of registration. In addition, Macmillan Cancer Support and Cancer Research UK have embarked on a rapid review to define a new approach to informing patients about cancer registration. They are involving people affected by cancer, NHS staff caring for them, cancer charities and other stakeholders including Public Health England and privacy campaigners. The Review looks forward to seeing progress in this vital area.

Exceptions and overrides

3.2.40 **As now, there are a limited number of specific circumstances in which an individual's decision to opt-out should not apply:**

(i) Where there is an overriding public interest, on a case by case basis, such as preventing and responding to natural disaster; monitoring and control of important diseases in humans such as TB and diseases of epidemic potential such as Ebola; infections that pass between animals and humans such as the zika virus; and for chemical, biological, radiological and nuclear events. The Review heard

CASE STUDY 11: Genomics England

Genomics England aims to sequence 100,000 human genomes from around 70,000 people to support better diagnosis and better treatments for patients and enable medical research. To do this they operate an explicit consent model, which makes it clear to participants that by agreeing to genomic sequencing they are also agreeing to the use of their information for medical research including by commercial organisations.

103. http://www.phgfoundation.org/file/17089/

evidence of the importance of the opt-out not applying to the monitoring and control of communicable diseases and certain other public health emergencies. **The Review suggests that the use of personal confidential data for monitoring and control of communicable diseases and other risks to public health[104] are not subject to an opt-out to ensure the safety of the public's health.**

(ii) **When information is required by law or by a court order. This includes the following examples:**

- the Care Quality Commission, which has powers of inspection and entry to require documents, information and records – a code of practice sets out how the CQC can use these powers[105] (Health and Social Care Act 2008);
- the HSCIC, the statutory safe haven, which has powers to collect information when directed by the Secretary of State or NHS England (Health and Social Care Act 2012);
- the NHS Counter Fraud Service, which has powers to prevent, detect and prosecute fraud in the NHS (National Health Service Act 2006);
- investigations by regulators of professionals (e.g. Health and Care Professions Council, General Medical Council, or Nursing and Midwifery Council investigating a registered professional's fitness to practise) (e.g. under the Medical Act 1983);
- coroners' investigations into the circumstances of a death, i.e. if the death occurred in a violent manner or in custody (Coroners and Justice Act 2009);
- health professionals must report notifiable diseases, including food poisoning (The Public Health (Control of Disease) Act 1984 and the Health Protection (Notification) Regulations 2010);
- the Chief Medical Officer must be notified of termination of pregnancy, giving a reference number, date of the birth and postcode of the woman concerned (Abortion Regulations 1991);
- employers must report deaths, major injuries and accidents to the Health and Safety Executive (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013);
- information must be provided to the police when requested to help identify a driver alleged to have committed a traffic offence (The Road Traffic Act 1988);
- information must be provided to the police to help prevent an act of terrorism or prosecuting a terrorist (The Terrorism Act 2000 and Terrorism Prevention and Investigation Measures Act 2011);
- information must be shared for child or vulnerable adult safeguarding purposes (e.g. s.47 Children Act 1989); and
- health professionals must report known cases of female genital mutilation to police (Female Genital Mutilation Act 2003).

HSCIC collecting data

3.2.41 The exceptions above set out when information is required by law – including the legal powers of the HSCIC to collect information when directed by the Secretary of State or NHS England. The Review looked at public opinion on HSCIC collecting data**.** In public focus groups, the Review heard that although HSCIC was not widely known, when information was provided people understood that it was part of the NHS 'family' and was seen as a trusted internal organisation[106]. The Review heard strong evidence, for example from statutory bodies, that flows of information to the HSCIC are important for ensuring that high quality linked data can be provided by HSCIC e.g., for running the health and care system. The Department of Health's current policy position allows people to opt out of their personal confidential data held by GPs being collected by HSCIC[107]. Applying this policy to all HSCIC data collections, including existing data collections from hospitals, would degrade the quality of data currently available to statutory bodies, researchers and local commissioners. **The Review recognises that the new opt-out should not cover HSCIC's already mandated data collections, such as Hospital Episode Statistics (HES) data. The Review believes it is important that there is consistency and therefore where there is a mandatory legal requirement for data in place, opt-outs would not apply.**

104. As authorised in regulation 3 of The Health Service (Control of Patient Information) Regulations 2002, SI No. 1438
105. http://www.cqc.org.uk/content/code-practice-confidential-personal-information
106. Public focus groups.
107. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251750/9731-2901141-TSO-Caldicott-Government_Response_ACCESSIBLE.PDF

Information for statistics

3.2.42 The Office for National Statistics (ONS) is the UK's largest independent producer of official statistics and is the executive office of the UK Statistics Authority, which is the recognised national statistical institute for the UK. It is responsible for collecting and publishing statistics related to the economy, population and society at national, regional and local levels. It also conducts the census in England and Wales[108].

3.2.43 Under the Statistics and Registration Service Act 2007, ONS can receive person level demographic information (in particular: date of birth; sex; NHS number; address and previous addresses; and primary care registration history) for the production of population statistics, which include internal migration. This excludes information about individuals' health and social care and the data that the ONS produces using this information is vital to the appropriate funding of local public services, among other uses. **For this reason, the Review has not made data flows into the ONS for the production of official statistics part of the proposed opt-out.**

Invoice validation for non-contracted activity

3.2.44 The Review also looked at the information needed to allow for payment of services, which commissioners had identified as an area where personal confidential data is required. Non-contracted activity refers to NHS funded services delivered to a patient by a provider, which does not have an agreed contract with the patient's responsible commissioner. For example, a patient may live in Bromley and be taken critically ill whilst on holiday in Devon. South Devon and Torbay CCG will send an invoice to Bromley CCG for the patient's care. Bromley CCG will want to check that they are responsible for the patient before paying the invoice.

3.2.45 NHS England estimates that CCGs process hundreds of thousands of non-contracted activity invoices per year, worth up to £1 billion. The proportion of patients that will opt out of the new model is unknown, but even a small percentage of opt-outs could represent a serious financial risk as without access to data about those that opt out, commissioners will be unable to validate non-contracted activity invoices relating to them.

3.2.46 During testing, members of the public did not express concern about their information being used for payment purposes. *'Overall there were no issues with this example of data sharing because the information is shared within the NHS – just one hospital to another'*. The law is not clear on whether personal confidential data can be used for these purposes without an opt-out. Taking into account the importance of accurately allocating NHS resources and the lack of evidence of public concern in relation to the use of data for this specific purpose, it is recommended that invoice validation for non-contracted activity should be an exception to the opt-out. The Department of Health should enable this through new regulations, which should be limited to when there is no alternative solution, such as the use of anonymised data. NHS England should continue to work on solutions which do not require personal confidential data. There should be further engagement with the public about how their information is used, including for payment, because this use of information whilst being broadly acceptable was 'new news'.

Recommendation 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.

Deceased patients

3.2.47 Where a patient has opted out, this should continue to apply after they have died unless the public interest served by the disclosure outweighs the public interest served maintaining confidentiality. The fact of a person's death is not patient confidential data and, therefore, would not be part of the opt-out.

Restrictions on disclosure

3.2.48 There are restrictions on the disclosure of some specific types of information. For example, the disclosure of 'protected information' under the Gender Recognition Act 2004 or information kept by clinics and the Human Fertilisation and Embryology Authority (HFEA) under the Human Fertilisation and Embryology Act 1990[109].

108. http://www.ons.gov.uk/ons/about-ons/index.html
109. Written evidence from the HFEA

3.3. Implementing the new opt-out model

3.3.1 **From recent public engagement it is evident that there is a low level of understanding of the health and social care system and how information is used. The Review recommends that the Department of Health conducts a formal public consultation on the proposed new opt-out model. It is important that this consultation is accessible to members of the public and is used to start an enhanced public dialogue about the use of information. Alongside the consultation, both the one-question and two-question models should also be tested with professionals and the public.**

3.3.2 **At the moment, there are a number of different opt-outs, including Type 1 and Type 2 opt-outs and other objections and opt-outs housed in national and local computer systems.** In September 2013 the Secretary of State for Health said: 'Any patient who does not want the personal data held in their GP record to be shared with the HSCIC will have their objection respected'. Two opt-outs were subsequently introduced: one for personal confidential data leaving the GP practice for purposes beyond direct care (Type 1), and the other for personal confidential data being disseminated from HSCIC aimed at purposes beyond their direct care (Type 2). In December 2015, the HSCIC started to collect data from general practices in England relating to patient objections. It began upholding those objections from the end of April 2016[110] [111].

3.3.3 **The Review is not recommending any changes to the existing arrangements until there has been a full consultation on the proposed new consent/opt-out model.** Both Type 1s and 2s should apply while the Department of Health conducts a formal consultation and further testing of both types of the questions proposed with patients and professionals.

3.3.4 **People have told the Review they want a simple explanation and choices that are clearer to understand. The Review is proposing a new model that has been designed to provide that simpler and less complex approach.** The HSCIC, as the statutory safe haven, can share data securely, and the public can have confidence in a simpler model. Once the consultation is complete, and the new model is in place, the past arrangements should be replaced. As part of managing this transition, the Department of Health should make sure it considers how to manage the objections already registered by patients both locally and nationally.

3.3.5 **The Review heard that people trust the NHS to handle their information securely and that they trust their GP in particular**. The Review also heard from GPs' professional bodies that they value the confidential relationship between doctors and patients. From patients it heard that they find the many different opt-outs that already exist confusing. This Review has benefited considerably from the advice and support of GPs and their professional bodies, as well as other health and social care professionals. In the next stage of the work, these groups should be asked how to support professionals to discuss the new opt-out and ensure that people's preferences are respected. There is a responsibility on professionals to ensure that they are providing information openly and respecting patients' own wishes.

3.3.6 **Work will also be needed to ensure that all registered providers, public bodies and other organisations participating in the health and social care system are in a position to implement the new consent/opt-out model. The size of this task should not be underestimated.** It would be good practice for information sharing choices to be discussed when a new patient registers at a GP practice. In addition, it should be made clear to patients that they can change their mind in the future and what they would need to do to change their preference.

3.3.7 This Review was not asked to look at care.data, although the pathfinder areas have been involved in shaping and testing the proposed consent/opt-out model, as have vanguards and health and social care integration pioneers. The consent and opt-out models proposed by the Review go further than the approach that was planned for the pathfinder areas, and should replace the approach that had been developed for those areas. The consent model should be tested in at least one pathfinder area, as well as in vanguards and integration pioneers. In the light of the Review, Government should consider the future of the care. data programme. The lessons learnt by the care.data programme and pathfinder areas should continue to be used to inform future developments.

3.3.8 On 15 December 2015, agreement was reached on new data protection rules, which mean that citizens will have the same data protection rights across the EU regardless of where their data are processed. The

110. http://www.hscic.gov.uk/article/7072/Applying-Type-2-Opt-Outs

111. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517522/type2objections.pdf

rules are set out in a new General Data Protection Regulation (GDPR) which has been adopted by the European Parliament and Council[112]. The GDPR will apply from 25 May 2018. Member states can, however, decide how they wish to regulate in a number of significant areas. There will be a two year transition period, and analysis of how the new framework is likely to impact on existing UK data protection legislation is underway, as is early policy thinking around implementation. The Department of Health will need to consider this during the implementation phase.

Communication

3.3.9 **Communication with the public cannot be viewed as a single event**. There is a risk that if the health and social care system does not communicate effectively with the public, people will rely on less reliable sources of information and public concern will increase, which could in turn impact upon participation. This could impact on the availability of data for important uses such as monitoring services that ensure safe care is being provided, and on the quality of research in the UK. The support and engagement of healthcare professionals in communicating how information is used is fundamental to the successful implementation of the new opt-out model. The review has developed two different models – there are a variety of ways that these could be presented and communicated to professionals and the public. One example which received positive feedback in workshops was a Facebook-style of 'preferences' model.

3.3.10 Our focus groups reflected evidence elsewhere that some members of the public feel uneasy about commercial organisations accessing information. The Review found that people are particularly concerned that if they allow their personal confidential data to be used they will be targeted by marketing or insurance companies. The Care Act 2014 introduced new protections which mean that the HSCIC can only disseminate information for the provision of health care and adult social care, or the promotion of health. It further makes clear that the HSCIC cannot disseminate data for solely commercial purposes such as for commercial insurance. In addition, the Data Protection Act 1998 provides protections more broadly against data being processed for any purpose that is incompatible with the original purpose for which it was collected. **Therefore the Review believes that is will be important that patients are given robust assurance that their data will never be used for marketing or insurance purposes.**

3.3.11 **Returning to the theme of trust, the Review heard consistently that the public want to understand who will have access to what data and for what purpose and how their personal confidential data will be protected.** Gaps in this information lead to public scepticism or fear.

3.3.12 The Health Research Authority publishes a list of applications which are approved under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002. However, this information is hard to find and may not be easily understood by a non-specialist audience. There are also no updates to indicate any benefits that have been achieved from using the data. Every organisation which processes information should ensure it has clear accessible information on how it uses information. Whilst the Review recognises that it is difficult to communicate the complexities of information sharing in the health and social care system, it should be easier for the public to access information about how data is used.

Recommendation 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.

Recommendation 18: The Health and Social Care Information Centre (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.

112. The Regulation is published in the Official Journal – http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

3.4. National Data Guardian's proposed consent/opt-out model

3.4.1 The Review has considered how the recommendations in this Section might be distilled into a set of eight statements that people could readily understand. The eight-point model is shown below.

3.4.2 It is followed by four different approaches that might be adopted when asking the public whether or not they wish to opt out from having information about them used for purposes beyond their direct care, such as checking the quality of care and researching better cures. The four options could be used to test whether or not the public would prefer a single opt-out, or two opt-outs distinguishing between using information about them to run services and using it for research. In each case there are two variants: asking people to choose an information profile that accords with their preferences; or asking them to tick a box when they want to opt out. These options are purely illustrative and the Review does not express a preference, or rule out alternative approaches. Extensive testing would be needed before asking people to make this important choice.

The eight-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 health care professional not to pass on particular information to others involved in providing your care.

3. Information is essential for other beneficial purposes.

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

4. You have the right to opt out.

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

This opt-out covers:

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

For example:

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

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

For example:

- a university researching the effectiveness of the NHS Bowel Cancer Screening Programme
- a researcher writing to an individual to invite them to participate in a specific approved research project
- a commercial organisation receiving data from an NHS organisation to look at whether contamination levels are safe for workers in the nuclear industry.

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

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

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

6. Explicit consent will continue to be possible.

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

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

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

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

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

8. 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).

Two question opt-out presented as an information profile

My health and social care information profile

People providing you with care need to know a certain amount about you to ensure that care is safe and effective. This personal confidential information about patients and service users is also useful for other purposes, such as checking the quality of care and researching better cures. You have a choice about how personal confidential information about you is used.

- ● **Standard setting – information about me can be used to run the NHS and social care system and to support research to improve treatment and care for everyone.**
  Your information will be used to check the quality of your care, to ask your opinion about the care you have received, and to help researchers improve how diseases such as cancer are treated and prevented.
- ○ **Limited setting – information about me can be used to run the NHS and social care system, but not for research.**
  Your information will be used to check the quality of your care and to ask your opinion about the care you have received. .Your information will not be used by researchers to improve how diseases such as cancer are treated and prevented.
- ○ **Restricted setting – information about me can only be used by the people directly providing my care.**
  People providing your care will be able to see the information they need. The NHS and social care system will not be able to use your information to check the quality of care you receive, nor will researchers use it to improve how diseases such as cancer are treated and prevented.

Your personal confidential information will only be used for purposes that benefit treatment and care. It will never be used for marketing or insurance purposes.

Two question opt-out presented with tick box

At the moment information about your healthcare is used when you are treated or given support by a health or care professional. That will continue.

People providing you with treatment and care need to know a certain amount about you to ensure that care is safe and effective. This personal confidential information about patients and service users can be useful for other purposes, such as checking the quality of care and researching improved treatment. You have two choices about how personal confidential information about you is used other than for your own care.

1. Allow my information to be used to support research to improve treatment and care.

This means:

- Researchers can improve how diseases such as cancer are treated and prevented
- Charities can evaluate the quality of services, for example for people living with dementia

If you agree you do not need to do anything.

If you do not agree, tick here ☐

2. Allow my information to be used to run the NHS and social care system

This means:

The NHS can ask your opinion about the care you have received

The NHS can check the quality of the care that you receive

If you agree you do not need to do anything.

If you do not agree, tick here ☐

Single opt-out presented as an information profile

My health and social care information profile

People providing you with care need to know a certain amount about you to ensure that care is safe and effective. This personal confidential information about patients and service users can be useful for other purposes, such as checking the quality of care and researching better cures. You have a choice about how personal confidential information about you is used.

- ● **Standard setting – information about me can be used to run the NHS and care system and to support medical research to improve treatment and care for everyone.**
  Your information will be used to check the quality of your care, to ask your opinion about the care you have received and to help researchers improve how diseases such as cancer are treated and prevented.
- ○ **Restricted setting – information about me can only be used by the people directly providing my care.**
  People providing your care will be able to see the information they need. The NHS and social care system will not be able to use your information to check the quality of care you receive, nor will researchers use it to improve how diseases such as cancer are treated and prevented.

Your personal confidential information will only be used for purposes that benefit treatment and care. It will never be used for marketing or insurance purposes.

Single opt-out presented with tick boxes

At the moment information about your healthcare is used when you are treated or given support by a health or care professional. That will continue.

People providing you with treatment and care need to know a certain amount about you to ensure that care is safe and effective. This personal confidential information about patients and service users can be useful for other purposes, such as checking the quality of care and researching improved treatment. You have a choice about how personal confidential information about you is used other than for your own care.

Allow my information to be used to run the NHS and social care system and to support research to improve treatment and care.
This means:

- Researchers can improve how diseases such as cancer are treated and prevented
- Charities can evaluate the quality of services, for example for people living with dementia
- The NHS can ask your opinion about the care you have received.

If you agree you do not need to do anything.

If you do not agree, tick here ☐

4. Next steps and implementation

4.1. Public consultation

4.1.1 This has been a short Review in which significant efforts have been made to take account of relevant evidence and involve as many people and organisations as possible. It has not been possible to address every issue in detail. For that reason the Review recommends that the Department of Health conducts a full and comprehensive public consultation on the proposed data security standards and proposed new consent/opt-out model. The Review also recommends that professional bodies and patient representative groups are further involved in testing and refining both the one and two-question models with the public and professionals. This consultation and testing must precede asking members of the public if they wish to exercise the new opt-out model. The consultation should be as full and open as possible.

4.1.2 Alongside this important engagement with patients and services users, it is also imperative that organisations whose work would be affected by the Review's proposals have the chance to respond to the recommendations during the consultation and are supported to prepare for implementation. This must include GPs and other care providers who will need to meet the new security standards, to explain data sharing and the opt-out to patients, and to honour the choices that those they are caring for have made. NHS and Local Authority commissioners must also be engaged: they will be required to take account of the data security standards when commissioning services and may need to change some of their business processes to rely less on personal confidential data and more on de-identified and anonymised data. Researchers, who may have concerns that the quality of the data they receive for some research projects is affected by citizens opting out, must also be included in the debate.

Recommendation 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.

4.2. Implementation

4.2.1 This has been a report about trust. It is hard for people to trust what they do not understand, and the Review found that people do not generally understand how their information is used by health and social care organisations. Engagement events with the public were particularly instructive in this regard: when longstanding elements of the current system for sharing information between health and social care professionals were described in workshops, the public tended to think they were hearing new proposals.

4.2.2 The question of implementation is beyond the scope of this Review. However, the engagement carried out during the evidence gathering phase highlighted a number of opportunities and issues that the Department of Health and its arm's length bodies should consider when embarking upon implementation.

The public

4.2.3 There should be ongoing work under the National Information Board (NIB) to look at earning public trust in the use of personal confidential data. The Review found that public understanding of the use and benefits of information sharing is limited – in particular there is a knowledge gap about the crucial need to share information across organisations to integrate health and social care. There is a need to ensure that the public have the information they need on new ways of working to manage expectations about their care, and the information sharing needed to

support care. The proposed public consultation on this Review's recommendations would be a good place to start this process.

4.2.4 The NIB should work with organisations and umbrella bodies from across health and social care to ensure that people are informed about how the health and social care system works. This should include informing people about new ways of working and the role of information sharing in integrated care; the importance of information sharing for running the heath and care system; and the value of information to support researchers to improve treatments and care[113]. It will be important to consider creative ways of communication, learning from best practice in social campaigning and behavioural insights, in order to fully engage all parts of the population, some of whom may only rarely use health and social care services. The Wellcome Trust has recently come forward with an offer to host an independent Taskforce looking at improving discussions about data. This could be a useful way of developing this work.

4.2.5 In communicating the value of data sharing for a range of purposes, there is a need to assure the public that their data is used appropriately and securely. The details of the processing and uses of data should be explained so that, for example, the public understand: the difference between anonymised and personal confidential data; where anonymised data can be used; and when personal confidential data is needed. The role of HSCIC and why it is important that HSCIC has access to information held by health and social care providers, in particular from GPs, also needs to be articulated. Finally, the discussion should be framed within the context of how information sharing in health and social care compares to data use in different sectors and the government's wider ambitions for the use of data.

Recommendation 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.

Professionals

4.2.6 Work is needed to consider how best to implement the mandatory data security standards in a way that creates a learning culture so that organisations are supported to meet the requirements. The Department of Health and its arm's length bodies should consider the incentives and levers, training, support, and communications needed. This may include an official launch and communications campaign, peer mentoring and peer review, incentives for compliance and sanctions for breaches, publicity about existing organisations set up to support professionals (CareCERT and CERT-UK's Cyber Security Information Sharing Partnership (CiSP)), model commercial contract templates, and procurement guidance. Formal accreditation of the standards should also be considered.

4.2.7 For implementation of the new consent/opt-out model, the Department and its arm's length bodies should consider the role of professionals in informing the public of their options. If social workers, GPs, nurses and other front-line professionals are expected to discuss the choices with people, the Department and its arm's length bodies will need to work with the relevant professional bodies to develop appropriate training materials and supporting information. The Review found that in primary care it was helpful to involve practice managers in discussing data sharing options with patients.

4.2.8 The Review heard the importance of having consistent messaging and guidance to support implementation. This is particularly problematic in social care, where the Review heard that different Government departments often convey different messages to social care professionals. The Department of Health should work with other government departments with responsibility for social care to ensure consistent messaging.

Technical implementation

4.2.9 The Department of Health should consider the recommendations set out for embedding the mandatory data security standards. Further work is needed to consider methods for tracking compliance and assuring the standards, and sanctions for non-compliance. The Department should consider the resource needed to support an internal and external audit function to monitor compliance, and for updating the IG Toolkit and IG training tool in line with the Review's recommendations.

4.2.10 The Review has worked with HSCIC and others to consider the technical implications for implementing the proposed new consent/opt-out model and substantive work is needed to scope the requirements. The Department of Health should consider how frequently, by whom and in what manner the model is presented to an individual and the opportunities for digital solutions.

113. The organisations consulted for this Review would be a good starting point for this work.

4.2.11 The Review recognises that implementing its recommendations may take time and that some organisations are not currently equipped to implement consent and opt-out preferences, for example. The Department of Health should look at this issue as part of implementation and should seek to find a mechanism to make it easy to register people's preferences and act upon them.

4.2.12 On data security specifically, the Review consulted with social care professionals and representative bodies. However, as the CQC's part of the review did not consider social care, further work is needed to establish the validity of the data security standards for this sector. This can be addressed through a full and comprehensive public consultation.

4.3. Conclusion

4.3.1 Beyond an understanding that patient records are used to help deliver direct personal care, the public's knowledge about how health and social care data is collected, protected, and used within the health and social care system is limited. It is therefore clear that future communications cannot make any assumptions about existing knowledge of data processes and uses, and that there is a role for all health and social care professionals to support public understanding.

4.3.2 There is a high degree of trust in NHS organisations to look after people's data and for health professionals to use it appropriately. Work is now needed to raise public understanding of the variety of organisations and agencies involved in delivering health and social care and to extend public trust across this system. The proposals set out in this report were designed to assure the public that their personal confidential data is secure and empower them to make informed choices about the use of that data.

4.3.3 As this report has noted throughout, use of data is essential to providing excellent care, to running a world-class health and social care system, to improving the quality of care and to support life-changing research. These important public benefits rely on data being shared with the relevant health and social care professionals and organisations. However, this sharing should not discount the interests of the individual – personal confidential data must always be protected properly, and shared on the basis of public trust.

Annex A. National Data Guardian's Review Terms of Reference

On 2 September 2015 the Secretary of State for Health, Jeremy Hunt, commissioned an independent Review to deliver by January 2016. The Review aimed to help address the following issues:

- As the use of technology increases, so does the need to reassure the public that their personal health and care data is being held and used securely.
- The health and care system has not yet earned the public's trust in this area and must be able to assure the security of confidential data.
- Being clear with citizens and professionals how personal health and care data should be used, and the benefits of doing so, how privacy is protected and the choices available to people to object to data about them being used.

Linking with CQC's Review of current approaches to data security across the NHS to prevent personal confidential data falling into the wrong hands, Dame Fiona Caldicott, the National Data Guardian Review was asked to:

Develop new data security standards that can be applied to all health and care organisations

Work up a set of new, easily understandable standards for the security of personal data, whether held on paper or electronically, that can be applied to the whole health and care system.

With CQC, devise a new method of testing compliance with the new standards

To ensure health and care organisations are held to account for their data security capability. In developing new standards, work with CQC to provide recommendations on how they can be assured, as appropriate, through CQC inspections and NHS England commissioning processes.

Propose a new consent/opt-outs model for data sharing

Develop a single question consent model which makes it absolutely clear to patients and users of care when health and care information about them will be used, and in what circumstances they can opt out.

Annex B. Members of the National Data Guardian's Panel

The National Data Guardian's Panel provided steers and oversight to the Review. Membership is as follows:

- Dame Fiona Caldicott – National Data Guardian and Chair, Oxford University Hospitals NHS Foundation Trust
- Ian Atkinson – Former Sheffield Clinical Commissioning Group, Healthcare Consultant
- Dr Joanne Bailey – GP, member HSCIC Data Access Advisory Group
- John Carvel – member, Healthwatch England National Committee
- Dr Alan Hassey – retired GP, HSCIC IG Clinical Lead & Deputy Caldicott Guardian
- Eileen Phillips, Freelance Writer, Communications Consultant
- Professor Martin Severs – University of Portsmouth, Caldicott Guardian and Lead Clinician, HSCIC
- Anne Stebbing – Consultant Surgeon, Caldicott Guardian, Hampshire Hospitals NHS Foundation Trust
- Dr Mark Taylor – University of Sheffield
- Richard Wild – Information Governance Consultant
- Chris Cox – Royal College of Nursing

The Review Team and Panel Members would also like to express deep gratitude for the work of Karen Thomson on the Information Governance Review (Caldicott2). Without her valuable contribution and insights the foundations for much of the present Review would not have been established.

Annex C. Organisations consulted during the Review

During the course of the Review the organisations consulted during the evidence gathering process were as follows:

- 38 Degrees
- Academy of Medical Royal Colleges
- Alstrom Syndrome UK
- Alzheimer's Research UK
- Apple Inc
- Arthritis Research UK
- Association of Directors of Adult Social Services
- Association of Medical Research Charities
- Association of the British Pharmaceutical Industry
- Asthma UK
- Big Brother Watch
- British Heart Foundation
- British Medical Association
- Cabinet Office
- Camden Council
- Cancer Research UK
- Care Quality Commission
- Centre of Excellence in Information Sharing
- Clinical Practice Research Datalink
- Cystic Fibrosis Trust
- Department of Health
- Department for Culture, Media and Sport
- Department for Education
- Department for Work & Pensions
- East and North Hertfordshire Clinical Commissioning Group
- Equality and Human Rights Commission
- Exabeam Inc
- Genetic Alliance
- Genomics England
- GlaxoSmithKline
- Government Communications Headquarters
- Government Digital Service
- Hammersmith & Fulham Council
- West Hampshire Clinical Commissioning Group
- Hampshire County Council
- Health and Social Care Information Centre
- Health Research Authority
- Healthcare Quality Improvement Partnership
- Healthwatch East Sussex
- Healthwatch England
- Healthwatch Lambeth
- Healthwatch Surrey
- Healthwatch Waltham Forest
- HM Revenue & Customs
- Human Fertilisation & Embryology Authority
- Hammersmith and Fulham Council
- IdenTrust
- Imperial College London
- Imperial College Healthcare NHS Trust
- Information Assurance for Small and Medium Sized Enterprises (IASME)
- Information Commissioner's Office
- Information Governance Alliance
- Involve
- Kidney Research UK
- Leeds City Council

- Leeds GCSX
- Leeds West Clinical Commissioning Group
- Leicester City Council
- Lewisham and Greenwich NHS Trust
- Liberty
- Local Government Association
- Local Government UK
- Macmillan Cancer Support
- MedConfidential
- MedeAnalytics
- Medical Defence Union
- Medical Protection Society
- Medical Research Council
- Medicines and Healthcare Products Regulatory Agency
- Midlands and Lancashire Commissioning Support Unit
- Mind
- MQ: Transforming Mental Health
- National Archives
- National Audit Office
- National Care Forum
- National Crime Agency
- National Institute for Health Research
- National Pharmacy Association
- National Survivor User Network
- National Voices
- NHS Choices
- NHS England
- NHS Improvement
- NHS National Services Scotland
- NHS South Commissioning Unit
- North West London Collaboration of Clinical Commissioning Groups
- Nuffield Council on Bioethics
- Palantir Inc
- Public Health England
- Richmond Group
- Royal College of General Practitioners
- Royal College of Nursing
- Royal College of Physicians of London
- Royal College of Psychiatrists
- Royal Statistical Society
- Sciencewise
- Skills For Care
- Society of Local Authority Chief Executives and Senior Managers
- South Central Ambulance Service NHS Foundation Trust
- Surrey County Council
- Sussex Partnership NHS Trust
- TechUK
- Templar Executives Ltd
- The Bank of England
- The Brain Tumour Charity
- The Health Foundation
- The Patients Association
- The Security Company
- The Security Awareness Special Interest Group
- TPP
- UK Council of Caldicott Guardians
- Wellcome Trust
- West Midlands Ambulance Service Foundation NHS Trust
- Westminster Council
- WhizzKids
- Yorkshire Ambulance Service NHS Trust

Annex D. The seven Caldicott Principles

Principle 1: Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

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 is transferred or accessible as is necessary for a given function to be carried out.

Principle 4: Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6: Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

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.

Annex E. Analysis of existing standards

In considering the introduction of a new data security standard, the primary task was to conduct a review of those standards currently used within the health and social care sector. In keeping with the emerging evidential themes of the Review, those standards in use were assessed in terms of: perceived effectiveness; ease of use; proportionality (the ability to scale effectively between providers of differing scale or complexity); financial cost; and resource burden.

Within the health and social care sector, a number of information assurance frameworks, standards and information governance processes were found to be in operation. These included: The Health & Social Care Information Centre's Information Governance Toolkit (IG Toolkit) and Information Governance Statement of Compliance (IGSoC), The Cabinet Office/CESG/CPNI/ BIS produced Cyber Essentials, Cyber Essentials PLUS, 10 Steps to Cyber Security, Cyber Streetwise website, and the Public Services Network – Code of Connection (PSN CoCo) operated by Government Digital Services (GDS). Also considered within the Review were commercially available standards operating within the wider public and private sectors, including; the internationally recognised ISO/ IEC27000:2013 series of Information Security Management standards and the Information Security Forum's Standards of Good Practice (ISF SoGP).

Public sector standards

The IG Toolkit is a mandatory governance process for all organisations operating within the health and social care sector. The Review found widespread awareness of the IG Toolkit amongst those consulted. In larger organisations, dedicated information governance staff are employed to manage their information governance frameworks and submit IG Toolkit assessments on behalf of the organisation. Smaller organisations do not necessarily have dedicated staff to work in this area. Instead, such tasks are usually allocated to management staff in addition to other governance duties. Often, such staff have a good appreciation of the requirement for confidentiality of data, but little expertise in broader information security topics (in particular the technical aspects), other than that gleaned from the IG Toolkit and its associated guidance and training.

The current version (13) of the IG Toolkit contains 24 different groups of requirements called 'views', each pertaining to different organisation types. Each 'view' features a different suite of 'requirements' to which the organisation must score their respective 'attainment levels'. The requirements are grouped into:

- Information governance assurance;
- Confidentiality and data protection assurance;
- Information security assurance;
- Clinical information assurance;
- Secondary use assurance;
- Corporate information assurance.

The allocation of requirements in differing tailored organisational views makes sector wide assessment difficult.

As IG Toolkit compliance is a largely self-assessed process, its practical effectiveness has proven difficult to evidence, although the incorporated Serious Incident Requiring Investigation (SIRI) tool, alongside mandatory reporting of serious breaches has provided significant insight into the types of events that have resulted in breaches of confidentiality. Less apparent from these reports are details of technical failures, or cyber security related events where the integrity or availability of data may be the key area of impact upon patient safety and the delivery of care services.

The IGSoC process has provided a means of assuring the security provision surrounding the technical infrastructure of potential service providers, although it is an additional, separate process from the IG Toolkit submission. Whilst the process provides some assurance that the provider organisations accessing nationally provided systems and services have appropriate security provisions in place, this is not

applied equally to NHS organisations that are already connected to the N3 network and have the necessary levels of access they require. This has created an unevenness of assurances within the sector, where NHS organisations are not obliged to provide assurances relating to the security provision implemented within their technical infrastructure. The Public Service Network – Code of Connection (PSN CoCo) process has been refined and simplified recently. The revised assurance model has been well received by the PSN community and compliance with the process has begun to increase significantly as evidenced by the Government Digital Service (GDS), which administers the process. This evidence suggests that a revised IGSoC process, perhaps also being incorporated into a refreshed Information Governance Toolkit platform may help raise compliance in a similar manner to that experienced within the PSN community. The imminent replacement of the current N3 contract may provide further incentive to support such a transition.

Cyber Essentials

The Cabinet Office in partnership with CESG (the Information Security arm of GCHQ), The Centre for the Protection of Critical National Infrastructure (CPNI) and the department for Business Innovation and Skills (BIS) has produced a number of freely available Information Security and Cyber Security related products and materials in recent years. These have been designed specifically to assist businesses in establishing and maintaining defences against the most common Internet related threats. The first product was published in 2012, entitled '10 Steps to Cyber Security'. This was well received by industry, raising levels of information security awareness amongst senior management within organisations and helping information security become a part of corporate risk management processes. Focusing upon key areas of vulnerability, the 10 Steps to Cyber Security guides organisations in developing information security controls tailored to their business needs and risk profiles.

Alongside the 10 Steps, a number of additional supporting documents were published, including:

- Executive companion;
- 10 Steps: Infographic;
- 10 Steps: A Board Level Responsibility;
- Advice sheets;
- Common Cyber Attacks and Summary report.

The 10 Steps to Cyber Security are now used by over two-thirds of the FTSE350 companies, and have been recognised as an effective means of raising awareness of cyber threats within the leadership of organisations, and to enable a greater capability to safeguard their most important information assets, such as personal data, online services and intellectual property. The 10 Steps to Cyber Security features controls to reduce risks in the following areas:

- Information Risk Management Regime;
- Secure Configuration;
- Network Security;
- Managing User Privileges;
- User Education and Awareness;
- Incident Management;
- Malware Prevention;
- Monitoring;
- Removable Media Controls;
- Home and Mobile Working.

By focusing attention on these key areas, organisations can bolster their defences against the most common cyber threats. Cyber Essentials can also be completed in parallel. Accreditation or certification against the Cyber Essentials standard is available via a community of CESG approved accreditation bodies.

The Cyber Essentials Scheme was published in 2013 to support the 10 Steps to Cyber Security in providing a standardised approach to assessing vulnerability and developing tailored mitigation strategies. Cyber Essentials is a cyber security standard aimed at organisations that are beginning the journey towards an enhanced, effective information security capability. The scheme focuses upon five key areas:

- Malware Protection;
- Secure Configuration;
- Access Control;
- Patch Management;
- Boundary Firewalls and Internet Gateways.

This focus ensures that the known threats presented by internet connectivity can be mitigated by the standardised implementation of control measures, limiting either the potential for security events to occur,

or the impact of an event should one occur. Cyber Essentials is evidential in nature and features audit criteria, upon which organisations can be independently assessed and certified (Cyber Essentials Plus), should the organisation wish to demonstrate certification to the standard. To date, only 13 organisations within the health and social care sector have completed Cyber Essentials.

Commercial standards

The ISO/IEC 27000:2013 series of standards is internationally recognised for its effectiveness in assisting organisations to implement and maintain effective information security management systems. The standards can be scoped to include all or parts of an organisation's security provision. The suite of standards covers all aspects of information security management, with separate detailed standards available to support the development of enhanced capability in specific areas, in line with the overall ISMS standard. The main standard covers the following 'domain' areas:

- Information Security Policies;
- Organisation of Information Security;
- Human Resource Security;
- Asset Management;
- Access Control;
- Cryptography;
- Physical and Environmental Security;
- Operations Security;
- Communications Security;
- System acquisition, development and maintenance;
- Supplier relationships;
- Information Security Incident management;
- Information Security aspects of Business Continuity management;
- Compliance; with internal requirements, such as policies and with external requirements, such as laws,

The 2013 version of the standard has been updated to reflect changes in technologies, such as cloud computing.

The ISO/IEC27000 suite of standards is currently not widely used within the health and social care sector, but those organisations which have implemented an information security management system in line with the standard have strengthened their capability to defend themselves against the most common types of threat from the internet. They will have greater ability to detect and respond to security events than those who have not acted similarly. Implementation, independent assessment and certification against the standards are typically conducted under contract with independent specialist consultants and accreditation service providers. Accreditation or certification against the standard is recognised as being relatively costly as the standards materials must be purchased and implementation usually requires the support of specialist consultancy. Certification assessments must be paid for and must be renewed every three years to remain valid.

The Information Security Forum – Standards of Good Practice (ISF SoGP) is an internationally renowned information security standard. Access to the standard is by subscription membership to the ISF, or by purchasing the materials directly from the ISF online store. The standard is possibly the most detailed currently available. The standard is reviewed annually to keep pace with changes in technology and the discovery of new vulnerabilities within systems and software, and the techniques by which attackers seek to exploit them. The ISF also contributed to the development of Cyber Essentials. The Standards of Good Practice is undoubtedly comprehensive in its scope, but for organisations with immature or untested information security capability, implementation would usually require external information security consultants, adding to costs.

Overview of standards

Product	Coverage	Utilisation	Strengths	Weaknesses
NHS Information Governance assurance processes	IG Toolkit • Mandatory for all NHS & provider organisations • Partial coverage of social care organisations where they wish to work with NHS organisations Information Governance Statement of Compliance • All third parties requiring N3 network access	Well established platform with good functionality, but inconsistent application at organisational level	• Database of contact details for IGT administrators • Good granularity in attainment level evidence requirements • Good focus on privacy and confidentiality aspects of care delivery and management • Comprehensive historical records • Extensive reporting and broadcasting capabilities	• Self-assessment provides limited assurances • Little compliance checking or audit of responses lessens assurance value • Little technical focus on NHS organisations may suggest a lack of import in this area • Seen by some organisations as a 'tick box' exercise • Language and vocabulary does not always align with security industry terminology
GESG standards	• 10 steps to cyber security • Cyberstreetwise • Cyber Essentials • Cyber Essentials plus – Focuses upon the 'essentials' providing a platform for continuous improvement	Small & Medium-Sized Enterprises in the UK	• Materials are free of charge • Supported by Confederation of British Industry (CBI), Federation of Small Business • Mandatory for suppliers involved with HMG procurements over a specified value • Highly acclaimed • More achievable	• Less detailed than ISO/IEC, ISF (SoGP) • Lesser awareness and existing compliance within International providers community • Cyber Essentials has very limited scope. Needs some contextual wrappers around it, to avoid misinterpretation/ confusion
ISO/IEC standards	• Information security management, risks and controls within the context of an overall information security management system (ISMS) • The series is deliverately broad in scope, covering more than just privacy, confidentiality and IT or technical security issues	Internationally recognised benchmark. In the health & care sector, certification is confined to a relatively small number of individual organisations	• Detailed, broad in scope • Scope can be tailored to suit organisational requirements, but better suited to larger organisations • Internationally recognised	• Expensive to obtain certification • Generally requires consultancy to complete • Time consuming to complete • Essentially, it's still self-assessment (especially if the scope is broad)

Annex F. Evidence and analysis

The Review wished to gain views from a broad range of individuals as well as an in-depth understanding of thinking around data security and consent to data sharing. Due to limited time available during the Review, a mixed approach to evidence gathering and analysis took place. The Review gathered primary evidence (both quantitative and qualitative), as well as reviewing academic literature and existing surveys on relevant topics.

Evidence gathered from these various methods is used throughout the report. A secondary stage of analysis has also compared the findings from the primary evidence to a review of the existing evidence not collected during the Review.

Primary evidence collected by the Review composed a range of evidence gathering and analysis methods. These included:

- Evidence sessions and interviews with key organisations;
- Focus groups with patients, GPs and social care providers;
- An online survey.

Gathering of existing evidence was also undertaken, including:

- Existing evidence on patient opinion;
- Models of consent in international healthcare;
- Existing models of consent in commercial organisations.

The Review also held four evidence sessions, each with groups of 15-25 individuals from the research community, social care, NHS Providers and patients, service users and carers. The sessions discussed the understanding of how personal data was being used, how consent models were currently being used, and how a new opt-out model should be constructed. Also discussed were the perceptions of data standards and how a new data standards model and system should be designed.

A further evidence session was held which focused solely on data breaches and data standards. A session was also held with the IT providers that provide systems to GPs and social care.

Eight focus groups with patients and the general public were led by the Review. Each group was designed to gain views from individuals with different characteristics (based on life stage, health status and economic status). The focus groups were held in various locations. The groups discussed current understanding of personal confidential data use in the NHS, how data could be used across differing organisations, and explored patients' views to a range of data sharing scenarios. A range of in-depth interviews took place with key interested organisations and individuals including NHS organisations, professional councils, government, charities and private organisations, providing more focused views on both data standards and consent.

Finally, written evidence from organisations into any views or studies they had undertaken which could inform the Review, was welcomed.

Summary of online survey findings

An online survey was publicised through networks of those who attended the Patients, Service User and Carers Evidence Session and on Twitter and received 416 respondents within the period the survey was open for one week.

The survey asked individuals about trust in certain organisations to keep their private healthcare information safe and secure, the organisations involved in sharing data and whether they would consent to sharing data for different purposes.

The main purpose of the survey was to inform the Review with views from patients, service users and the public. The survey results sit within a larger section of analysis which looks at a wider group of people than the small sample of this study. Due to the nature of the survey, the circulation method, respondents and respondent numbers the survey may not be representative of the views of the wider population.

Organisational trust

Individuals were asked, how well they trust the NHS organisations to collect, process and use information about themselves safely and securely. The same question was also asked about social care organisations. Responses were gathered on a scale of 1 (not at all) to 5 (very much.)

Overall there was a higher level of trust in the NHS (average 3.1) than in social care organisations (average 2.7), although the difference between the sectors was not substantial.

A further question asked respondents about which organisations and professionals they trusted to collect, process and use information about themselves safely and securely. Only the individuals' GPs were trusted by more than half of respondents (83%). The Health and Social Care Information Centre (35%) and research organisations (29%) were the next most trusted, followed by care workers (14%), pharmaceutical companies (12%) and other commercial organisations (7%).

Purpose of sharing data

Respondents were asked whether they were happy for information about themselves to be used to support direct care with 1) a GP/hospital and 2) social care organisations.

Respondents were generally in favour of information being shared for direct care purposes with a GP or a hospital (84% responded positively). For information sharing with care homes, a smaller majority showed support (58% positive).

The survey also asked about whether respondents would support sharing data for purposes beyond direct care. It asked whether respondents would share their data for the following five purposes: NHS local planning, checking the quality of care, clinical research, government policy development and public health reasons. Respondents were given the options of saying that they supported data sharing (yes, yes if anonymised, and yes if asked first), or that they opposed sharing.

Generally there was support for data being shared beyond direct care, particularly if the data is anonymised, with the highest levels of support for sharing information for NHS purposes. 74% were happy for their data to be shared to support NHS local planning (18% said yes and a further 56% said yes, if the data was anonymised). A further 13% per cent said they would be happy, provided they were asked first.

Sources of information on data sharing

Respondents were also asked where they expected to find information about data use and data security. Options included NHS and social care sites, online and via friends and family. Over half of respondents chose gov.uk (74%), the GP practice (73%)and NHS choices (67%) over other places as where they would most expect to find information about data use and security.

Survey respondents

The online survey had 416 respondents. Not all respondents answered every question; with the most skipped question having 64 non-responses.

The majority (55%) of survey respondents were aged 55 and over. When asked about which group most accurately applies to themselves, a majority (69%) were patients or service users with a long term condition or disability, while 11 % identified themselves as a carer, 2% as a retired health care professional and 15% as an interested member of the public. The large majority (97%) of respondents were of white ethnicity.

The following table summarises responses to this question:

	Yes	Yes, if anonymised	Yes, if asked first	No	I'm not sure
NHS local planning	18%	57%	13%	10%	2%
Check Quality of Care	16%	56%	14%	11%	2%
Clinical Research	18%	48%	18%	14%	3%
Public Health	14%	51%	14%	17%	4%
Government policy development	13%	49%	15%	19%	5%

Annex G. Summary of terms used in the report

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.

Cloud services: Any resource that is provided over the internet.

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.

Cryptography: A discipline which embodies principles, means and methods for the transformation of data in order to hide their information content, prevent their undetected modification and/or prevent their unauthorised use [ISO 7498-2:1989, definition 3.3.20].

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'.

General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) is the new EU Regulation 2016/679 adopted by the European Parliament and Council, which is intended to strengthen and unify data protection for individuals within the European Union.

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 (IG): The set of multi-disciplinary 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 (IG 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.

Integrated Care Pioneers: Local areas covered by a Clinical Commissioning Group, Local Authority, or larger area which work across the whole of their local health, public health and care and support systems and with other Local Authorities to achieve and demonstrate the scale of change needed.

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.

N3: The national broadband network for the NHS in England.

NHS Vanguards: Sites taking the lead on the development of new care models as laid out in the Five Year Forward View.

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 this 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.

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.

Senior Information Risk Owner (SIRO): An Executive Director or member of the Senior Management Board of an organisation with overall responsibility for an organisation's information risk policy.

Serious Incident Requiring Investigation (SIRI): Formerly known as Serious Untoward Incident. Any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals is regarded as serious. The severity of the incident determines the action to be taken following the incident.

Smartcard: Similar to a chip and PIN credit or debit card, but more secure. A Smartcard controls who has access to a particular computer system and what level of access they can have. An NHS Care Records Service user's Smartcard is printed with their name, photograph and unique user identity number.

2904918 June 2016
Prepared by Williams Lea for The National Data Guardian