Rt. Hon Jeremy Hunt MP
Secretary of State for Health
Department of Health
Richmond House
79 Whitehall
London SW1A 2NS

6 July 2016

Dear Secretary of State,

Last September you asked the Care Quality Commission (CQC) to undertake a review of data security in the NHS, and in parallel for Dame Fiona Caldicott, the National Data Guardian, to develop new data security standards and a method for testing compliance against these. You also asked Dame Fiona to recommend a new consent model for data sharing in the NHS and social care. You highlighted the importance of us working closely together and today we are pleased to publish our reports.

There are strong common themes between our findings and recommendations. Both reviews found that across the NHS there is widespread commitment to keeping data secure and that the public generally trusts the NHS in particular to do so. We also heard that processes work best when they are designed to support staff in delivering excellent care.

However, we have identified areas where more can be done to protect against potential risks. In May, we wrote to NHS trusts to highlight some of the key principles for good data security that arose from our reports, as well as immediate actions that could be taken in order to continue the important work of securing data.

We know that good information underpins good care, and that patient safety can only be assured when information is accessible, accurate and if confidentiality is maintained. We have made a number of recommendations to you. The National Data Guardian also proposes data security standards and a consent / opt out model for full consultation and further testing with the public. She also recommends that there should be a comprehensive dialogue with people about the benefits of data sharing.

Data security review findings

CQC's review of 60 hospitals, GP surgeries and dental practices focused on the availability, integrity and confidentiality of data systems in the NHS. Specifically, it found that:

- There was evident widespread commitment to data security, but staff at all levels faced significant challenges in translating their commitment into reliable practice.
- Where patient data incidents occurred they were taken seriously. However, staff did not feel that lessons were always learned or shared across their organisations.

- The quality of staff training on data security was very varied at all levels, right up to Senior Information Risk Owners (SIROs) and Caldicott Guardians.

- Data security policies and procedures were in place at many sites, but day-to-day practice did not necessarily reflect them.

- Benchmarking with other organisations was all but absent. There was no consistent culture of learning from others, and we found little evidence of external checking or validation of data security arrangements.

- The use of technology for recording and storing patient information away from paper-based records is growing. This is solving many data security issues but, if left unimproved, increases the risk of more serious, large-scale data losses.

- Data security systems and protocols were not always designed around the needs of frontline staff. This leads to staff developing potentially insecure workarounds in order to deliver good, timely care to patients – this issue was especially evident in emergency medicine settings.

- As integrated patient care develops, improvements must be made to the ease and safety of sharing data between services.

In carrying out the work to develop new data security standards for health and social care, the National Data Guardian's review found that:

- There is a high degree of public trust in the NHS to safeguard people's data. People want reassurance about security when data is being moved outside the NHS, and some want harsher sanctions for intentional or malicious breaches.

- GPs and social care professionals want a simple explanation of what they should and should not be doing and reassurance that organisations with which they share data are also protecting patient information.

- Previous information breaches mostly related to paper records, or to older equipment such as faxes. As the health and social care sector becomes more digital, many of these issues will be addressed automatically. However, as systems became more digital, breaches could affect greater numbers of people and the external cyber threat is becoming a bigger consideration.

- A number of data standards already exist, but data controllers are often unsure which to follow.

- Strong leadership, in particular from Senior Information Risk Owners (SIRO) and properly supported Caldicott Guardians, makes a significant difference.

- Integration is driving more data sharing between health and social care organisations, although a lack of understanding of security issues is causing people to default to risk avoidance and to be unwilling to share.

- Data breaches were caused by people, processes and technology, with people primarily motivated to get their job done and often working with ineffective processes and technology.

The National Data Guardian proposes ten new 'data security standards' for consultation. She recommends that leaders of all health and social care organisations commit to the standards, and demonstrate this through audit to support inspection.

Consent / opt-out review findings

In developing the proposed new consent / opt-outs model, the National Data Guardian Review found that:

- Trust is essential and should underpin any opt-out model. While 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.

- Both patients and professionals want clear communications about how professionals can and should share information.

- People's opinions on their personal confidential data being shared are influenced by the purpose for which it would be used. For example, there was concern about personal confidential information being used for insurance or marketing. In general, people were content with their personal confidential data being used for their own care.

- Information is essential to support excellent care, for running 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. But for the majority of purposes personal confidential data is not required. High quality, linked data that is anonymised will often be sufficient.

- There are some purposes where personal confidential data is needed: for example, for some planning, to check the quality of care, and for some research. People tend to support such uses, although they expect to be able to be asked about these purposes.

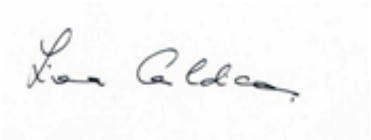
The National Data Guardian proposes a new consent / opt-out model for consultation to enable people to opt out from their personal confidential data being used for purposes beyond their direct care, including in running the NHS and care system and to support research to improve treatment and care. It is based on the purposes for which the data will be used. People should also be able to continue to give their explicit consent for specific research projects, as they do now. She proposes that the new model should be implemented by every organisation processing health and social care information. Ultimately, a person should be able to state their preference once (online or in person) and be reassured that this will be applied across the system. If they change their mind, that should be respected.

The National Data Guardian recommends that there needs to be a much more extensive dialogue with the public about how their information will be used, and the benefits of data sharing for their own care, for the health and social care system and for research. She suggests that there should be a full consultation on her proposals, as a first step in beginning that debate.

Our recommendations to you are attached. Given the close alignment of our reviews on data security, three of the recommendations are identical. Data security and consent should be treated very seriously. Whilst for the most part, personal data is generally managed securely in the NHS, organisations must show leadership in prioritising its accessibility, integrity and confidentiality, and ensuring that the security of data systems is proactively and regularly tested.

Yours sincerely,

David Behan
Chief Executive, CQC



Dame Fiona Caldicott, MA FRCP FRCPsych
National Data Guardian

Recommendations

CQC and the National Data Guardian are making the following recommendations to the Secretary of State. Given the close alignment between the work on data security, three of the recommendations are identical.

Data security [CQC and NDG]

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. [CQC and NDG]**

2. **All staff should be provided with the right information, tools, training and support to allow them to do their jobs effectively, while still being able to meet their responsibilities for handling and sharing data safely. [CQC]**

3. **IT systems and all data security protocols should be designed around the needs of patient care and frontline staff to remove the need for workarounds, which in turn introduce risks into the system. [CQC]**

4. **Computer hardware and software that can no longer be supported should be replaced as a matter of urgency. [CQC]**

5. **Arrangements for internal data security audit and external validation should be reviewed and strengthened to a level similar to those assuring financial integrity and accountability. [CQC and NDG]**

6. **CQC will amend its assessment framework and inspection approach to include assurance that appropriate internal and external validation against the new data security standards have been carried out, and make sure that inspectors involved are appropriately trained. [CQC and NDG]**

7. **HSCIC should use the redesigned IG Toolkit to inform CQC of 'at risk' organisations and CQC should use this information to prioritise action. [NDG]**

8. **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. [NDG]**

9. **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. [NDG]**

10. **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. [NDG]**

11. **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. [NDG]**

12. **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. [NDG]**

13. **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. [NDG]**

Consent / opt-outs [NDG review]

14. **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.**

15. **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.**

16. **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.**

17. **The Government should consider introducing stronger sanctions to protect anonymised data. This should include criminal penalties for deliberate and negligent re-identification of individuals.**

18. **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.**

19. **People should continue to be able to give their explicit consent, for example to be involved in research.**

20. **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.**

21. **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.**

22. **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.**

23. **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.**

24. **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.**

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.

The eight-point opt-out 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 body 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 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).