Care Quality Commission

Safe data, safe care

Report into how data is safely and securely managed in the NHS

JULY 2016

The Care Quality Commission is the independent regulator of health and adult social care in England.

Our purpose

We make sure health and social care services provide people with safe, effective, compassionate, high-quality care and we encourage care services to improve.

Our role

We register care providers. We monitor, inspect and rate services. We take action to protect people who use services. We speak with our independent voice, publishing regional and national views of the major quality issues in health and social care.

Our values

Excellence – being a high-performing organisation
Caring – treating everyone with dignity and respect
Integrity – doing the right thing
Teamwork – learning from each other to be the best we can

Contents

Foreword

Good information underpins good care.

Patient safety can only be assured when information is accessible, its integrity is protected against loss or damage, and confidentiality is maintained.

Data security should be treated very seriously. It has been an issue of national concern in the health sector for some years, but has now been pushed to the forefront of the public's attention by a number of recent, high profile data breaches.

Reflecting the importance attached to data security, the Secretary of State for Health asked CQC to do two things:

1. Review the effectiveness of current approaches to data security by NHS organisations when it comes to handling patient confidential data, and make recommendations on how current arrangements for ensuring NHS providers protect personal data could be improved.
2. Make recommendations about how the new guidelines (published by the National Data Guardian, Dame Fiona Caldicott) can be assured through CQC inspections, NHS England commissioning processes, and any other potential mechanisms.

The National Data Guardian was asked, as one aspect of the CQC-led review, to develop new data security standards that can be applied to all health and care organisations and, with CQC, to develop a method of assuring these new standards, as appropriate. Dame Fiona Caldicott was also asked to make recommendations on a new consent model for sharing patient information; informing the public how their data will be used and when they can opt out.

In our review, we found that across the NHS there is widespread commitment to keeping data secure, but effective action is not always being taken where necessary. While data, for the most part, is generally treated safely, NHS organisations remain vulnerable to potential risks.

We are clear that present data security systems and processes need to be continuously and actively reviewed so that they are resilient to current and future risks.

We have been reassured to find, through this work and data recorded by the Health and Social Care Information Centre, that there have been very few attacks on health information systems. Those that have occurred have targeted financial, not patient, data. In addition, the total number of reported data breaches is proportionately very small: there were 533 in the year to 31 May 2015, in the context of 6.5 billion data transactions (excluding paper transactions) across the whole NHS network in the same period.*

Even so, the review has found many instances of poor practice, any of which could have led to a data breach.

Complacency cannot be afforded. As confidential data is held and accessed in fresh ways through new technology, the risks change and so must the response if both security and public trust are to be maintained.

NHS organisations must take steps to understand their individual exposure to risk, and act to reduce it as a matter of priority.

There is a real need for the leadership of NHS organisations – from the lead partner in a small GP or dental practice to the chief executive and the board of a hospital trust – to prioritise the safety and confidentiality of personal data, and ensure that the security of data systems is proactively and regularly tested. Having the right policies in place is not enough – policies must be tested, much like the frequent checks of fire alarms and practising the full evacuation of a building. The leadership of all NHS organisations needs to demonstrate clear ownership and responsibility for data security, just as they should for clinical and financial management and accountability.

Importantly, there should be no conflict between protecting and sharing data. While data must be handled securely, safety barriers must not prevent information from being shared.

We are very grateful to all those who enabled us to conduct this review – we visited 60 NHS sites across England, and staff at all levels in those organisations gave their time to help us gather the data on which our work here is based. The generosity shown by healthcare staff, who shared their experiences and concerns, not only helped us in this piece of work - it will also enable the entire system to learn from their insights and so improve.

David Behan
Chief Executive

*All transactions across the NHS Spine, including 465 million NHS staff accessing and recording patient data, 193 million choose and book or e-referral transactions by patients.

Summary

This thematic review of data security was conducted to establish whether personal health and care information is being used safely and is appropriately protected in the NHS.

The review focused on patient data in the NHS (we were not asked to include providers of adult social care). We did not look at other areas of sensitive information such as HR or finance. We also excluded a detailed examination of IT systems, which was the subject of separate work carried out by the Health and Social Care Information Centre (HSCIC).

Data security, in this review, is defined as:

- **Availability** – how patient information is available to all those who need it to provide care where and when it is needed.
- **Integrity** – how patient information is protected from unauthorised alteration, damage and loss.
- **Confidentiality** – how patient information is kept confidential: safe from access by those without authorisation to read, see or hear it.

We gathered the evidence for this review by conducting staff interviews, observing practice and examining documentation in NHS hospitals, GP surgeries and dental practices. We also asked staff in the sites we visited to take part in a confidential online survey, reviewed relevant literature, consulted an expert panel of stakeholders and talked to individual experts in the field.

Common to all sectors and sizes of organisation was the range of human behaviours that could inadvertently lead to data breaches. As an example, a large hospital with diverse systems faced more difficulties than single-handed GPs, who were only working with a single system and were therefore less likely to have to log in and out of different systems to complete a single task. As a result, such a GP practice was less likely to invent the kind of insecure workarounds that we found in emergency care in large hospitals. However, some small primary care practices were working with outdated, unsupported technology, and did invent their own insecure workarounds in response to the challenges they faced, for example, taking home a system back-up in their bag, instead of backing up to a secure cloud (network of servers) or other secure mechanism.

Key findings

In the NHS organisations we reviewed, we found:

- 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.

Successful data security demands engaged leadership and a culture of learning and sharing. Senior leadership teams must take data security seriously and ensure clear responsibilities for all members of staff.

The recommendations set out in our report are detailed and apply to all health care settings. They can be summarised as follows:

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.

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.

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.

Computer hardware and software that can no longer be supported should be replaced as a matter of urgency.

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 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.

Introduction

Information, whether in paper or digital form, is critical to NHS patient care. The reason NHS organisations need to gather and hold information is to use it – both to treat and care for patients, and to improve the quality and efficiency of services.

Using information so that patients get the best care possible means sharing it with staff and with other providers of care (for example, an ambulance crew, a local GP, a care home or a specialist in another hospital).

When patient information, such as medical history, is not available to healthcare professionals, delays in treatment can occur. It is, therefore, vital that information systems ensure that patient information can be shared quickly, reliably and securely.

The use of technology for managing patient data is growing. But without robust processes and adequate IT systems, the integrity of information will be at risk of being compromised by unauthorised parties, it may not be accessible where or when needed, and it may not be kept confidential.

The financial cost of data breaches can be substantial and often more costly than prevention. In one such breach, arising from a web link in an unsafe email, the cost of repair to a hospital trust reached over £700,000. While some financial institutions set aside money to recover from data breaches, the NHS covers such incidents with funds intended for patient care and healthcare improvements. The cost to patient privacy and consequent loss of public trust can also be very substantial.

In line with our purpose to make sure care services provide people with safe, effective, compassionate, high-quality care, and to encourage improvement, the Secretary of State for Health asked CQC to review the effectiveness of current approaches to security by NHS organisations when it comes to handling confidential patient information. We were asked to make recommendations on how current arrangements can be improved and how new standards set by the National Data Guardian can be assured through CQC inspections, NHS commissioning processes and any other potential mechanisms.

This study provides a picture of the way in which NHS organisations approach the issue of data security.

In relation to data security, we have identified good practice, explored challenges in the NHS, and recommended how barriers to achieving excellence can be overcome.

The agreement from selected providers to participate in this review was invaluable in allowing it to be carried out within the timescale required. All were offered support by the Health and Social Care Information Centre (HSCIC) to make improvements where opportunities for doing so were identified. We have not attributed any findings to individual providers in this report and our findings do not contribute to the future ratings of any participating organisation.

How we carried out the review

We carried out the review between October and December 2015. The fieldwork was conducted by the Health and Social Care Information Centre (HSCIC) and its contractor, QinetiQ (a specialist in data security).

We identified 60 NHS provider sites across England to be included in the review, covering NHS trusts, independent GPs and dental practices, as well as GPs and dental practices that are members of large networks. We ensured that the sample was balanced by sector, size of organisation, the information we held through our existing inspections, and geography. We excluded providers that were undergoing comprehensive or responsive CQC inspections at the time of the review, to avoid interfering with CQC's ongoing programme of inspections. The sample consisted of:

- 18 NHS trusts:
  - Acute trusts (8)
  - Mental health trusts (4)
  - Community trusts (4)
  - Ambulance trusts (2)
- 22 GP practices
- 20 dental practices.

The GP practices we visited included those using a range of the most common IT systems. The dental practices included independent providers and those who were part of a group or chain.

All sites were checked against HSCIC records to see whether they had potentially been exposed to a particular cyber vulnerability in 2015. We used this measure to ensure that we included both sites that had been affected and those that had not.

Between 9 and 21 November 2015, research teams visited 60 NHS sites and conducted interviews and focus groups with more than 200 members of staff. They also explored how systems were used to store, access and share patient confidential data without compromising security.

The review focused on patient data in the NHS (we were not asked to include providers of adult social care). We did not look at other areas of sensitive information such as HR or finance.

The teams reviewed documents relevant to each organisation's data security, such as plans, policies, training materials, audits of data security, records of breaches, records of follow-up and patient leaflets. They also observed what staff did and how it could affect data security to corroborate the evidence gathered.

The research teams typically consisted of a technical expert from HSCIC, and an expert

in workplace behaviour and its effect on data security from QinetiQ. Some visits also included a member of the CQC project team.

In addition, we collected data from an online survey conducted by QinetiQ. This survey probed the extent to which staff understood their responsibilities for data security, their knowledge of policies and procedures, whether they had ever been put under pressure to break procedure, if they had witnessed any data security breaches, if they knew how to raise concerns, and the extent to which they felt confident in reporting concerns to senior management.

We also took part in a number of evidence sessions organised by the National Data Guardian team. This included one on the patient's perspective, and one that discussed the nature of recorded data security breaches in the NHS to date. We have used the findings from those sessions to inform our work and this report.

The review was shaped and supported by an expert reference group in September 2015, after which members of the group offered advice on the research assessment framework. The group reconvened in mid-December at a symposium jointly held with the National Data Guardian to test respective findings and explore recommendations.

As the technical experts in this field, HSCIC worked closely with CQC to shape the research, ensuring that the assessment framework drew on the requirements of the **Information Governance Toolkit** (IG Toolkit) and the **Cyber Essentials Scheme**.

INFORMATION GOVERNANCE TOOLKIT

The IG Toolkit is an online system that allows 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.

CYBER ESSENTIALS

The Cyber Essentials Scheme has been developed by Government and industry to fulfil two functions. It provides 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. And through its assurance framework it offers a mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions.

Our review also built on existing literature on data security and the findings from work conducted by HSCIC in 2014 (unpublished). The report included formal testing of NHS data systems to the extent to which unauthorised personnel could access secure IT systems physically or electronically.

We also took into account the **2015 Information Security Breaches Survey** conducted for the Government by PricewaterhouseCoopers and Info Security Europe across private and public sector organisations in different fields, **Ponemon Institute's work from 2012,** which looked at the human factor in data protection, work by the Information Commissioner on past data breaches and their origins in the NHS, and previous work carried out by QinetiQ.

We have sought to build on existing findings, adding new material to the growing body of knowledge. In particular, we have examined the managerial and organisational arrangements for data security, and the interaction between staff behaviours and data system design and operation.

Assessment framework

We used a detailed assessment framework to structure the interviews and discussions with staff. It was informed by, and linked to, the IG Toolkit.

Our assessment was structured around three key questions.

1. How well does the organisation's leadership enable staff to keep patient confidential information secure?
2. How well do the organisation's processes ensure the right levels of security of patient confidential information?
3. How well does the organisation equip itself with paper record keeping systems, hardware, software and IT updates to a standard suitable to ensure security of patient confidential information?

Within each of these three key questions we used a set of key lines of enquiry to consistently structure our review questions and evidence gathering.

Findings

Existing evidence

Ensuring that personal data is collected, stored, used and shared securely is an essential part of good care. This is a significant challenge for the NHS in terms of its operation, the changing environment in which health care is delivered, associated changing expectations of data sharing, and in light of the potentially significant consequences for patient care and patient confidence of any data breach.

Data held by the Health and Social Care Information Centre (HSCIC) and Information Commissioner's Office (ICO) shows the scale of digital data transactions. In the year to 31 May 2015, there were:

- 6.5 billion data transactions, such as people and organisations accessing, adding to, amending, sending, storing or sharing electronic data across the whole NHS network. The number of paper transactions is not known and therefore not included.
- 465 million transactions involving NHS staff accessing, logging and sharing data.
- 193 million 'choose and book' (or 'e-referral') transactions made by patients and staff.
- 533 reported incidents that were potential breaches of the Data Protection Act or Common Law Duty of Confidentiality, the majority of which concerned paper records not electronic data.
- Also, between September and November 2015, almost 848 million emails were received into the secure NHS system. Of these, 433 million were removed by system scanning tools at both the overall and local levels – more than half the emails received by the network.

The 533 reported breaches amounted to just over one for every million transactions involving staff, and far fewer for every million data transactions across the whole NHS network. Despite the very low ratio, every breach had the potential to have a huge impact on the individuals affected.

It is mandatory for the NHS to report incidents to the ICO. The majority of data breaches are related to paper records handled by NHS staff. These breaches are a cause for concern, but typically they affect relatively low numbers of individuals, in contrast to the number of people who would be affected by a significant breach of electronic data. This is why the review has focused on the nature, not the number, of breaches.

Evidence suggests that NHS patient data is not currently the highest priority for targeted attack by cyber criminals and hackers. There can be no certainty that this will not change. Incidents in the NHS mainly involve opportunistic 'botnets' (which can send out large amounts of spam email) and adware/spyware introduced by staff unwisely clicking on links in emails or using insecure browsers on NHS networks.*

American healthcare organisations are increasingly deliberately targeted by criminal cyber attacks seeking the financial details of patients and insurance companies. While this has not yet been widely observed in the NHS, it might also be at risk of such attacks in the future where such information is held. Few systems are 100% secure all of the time. Processes, systems and networks are only as strong as their weakest link, and often the weakest link arises as a result of error, misjudgement, and a culture where data security is not owned by the leadership of the organisation.

The last line of defence of any system, therefore, is the care and vigilance of staff using the system, supported and directed by the leadership of the organisation.

EXAMPLE

The Information Commissioner's Office (ICO) reported that an HIV patient network sent out a newsletter by email to 200 patients and put their email addresses in the 'to' field rather than the 'bcc' field. On receiving the email, the recipients could see all the individual email addresses, 56 of which contained full or partial names.

The incident was the second of this type at the network in three months. The ICO carried out an investigation and fined the network.

HSCIC's detailed IT Health Check Strategic Data Assurance Report in 2014 found that, while most aspects of cyber security were taken seriously and robust systems were generally in place, there were six areas where they recommended improvements:

1. Secure configuration of hardware and software.
2. Continuous vulnerability assessment and response.
3. Controlled use of administrative privileges to areas relevant to role.
4. User account monitoring and control to ensure compliance with policies in place.
5. User education and training on IT and data security.
6. Access control to IT systems for staff and contractors.

HSCIC judged that the first two of these weaknesses could have been addressed by the rigorous and timely application of patches (pieces of software designed to fix or improve data issues) that are routinely issued to NHS organisations. The remainder could have been addressed through more rigorous management of systems, and support to staff.

These measures would give NHS providers a simple and cost effective fix available to all NHS organisations using systems still supported by the IT industry. However, the patches issued are of no use to organisations that continue to use old hardware and software despite their known weaknesses and vulnerabilities (for example, Windows XP or old internet browsers).

*www.symantec.com/content/en/us/enterprise/other_resources/b_Financial_Attacks_Exec_Report.pdf

Data security review

The findings of the HSCIC and others shaped the focus of our assessment framework, leading us to look in detail at the underlying causes of risk. Estimates suggest that 80% to 90% of all data breaches concerning paper and electronic data are as a result of human behaviour – or 'non-malicious' incidents. This includes clicking on unsafe links in emails and accidentally losing storage devices (for example, memory sticks). The untargeted sending of unsafe emails is nevertheless a malicious act, one where the effects can be very greatly reduced by system filters blocking them from staff inboxes, as well as informing staff not to open or click on any emails of uncertain origin.*

Non-malicious internal incidents, however accidental, can introduce potentially damaging malware, such as computer viruses, into an otherwise secure IT system, making the task of securing an information system much harder.

Some of the actions we saw evidence of, or were told about, that could result in data breaches caused by human behaviour, included:

- Paper notes being lost on and off site, for example in staff belongings, left on wards or when patients were transported.
- Bagged confidential paper waste left unattended outside a building.
- Paper records left visible for unauthorised people to see, for example on trolleys in corridors, on unattended receptionist desks, or on trains and in cafes where staff were working between appointments.
- Emails sent to the wrong people.
- Faxes received by the wrong people.
- Fax machines left unattended in public areas when highly sensitive notes were being transmitted.
- Smart cards (programmed devices which give data access as necessary to carry out particular roles) being shared in the absence of sufficient supplies, for example when agency staff arrived for a shift, the lack of smart cards meant that staff going off shift had to lend theirs.
- Smart cards and user privileges not being withdrawn when staff left the organisation.
- Passwords written on sticky notes above computer screens.
- Coded door locks where passcodes had never been changed, doors wedged open, or pass codes written above door locks.
- Storage devices and smart cards lost.
- Unencrypted devices being used.
- Unfiltered browsing permitted, potentially allowing malware into the system.
- Passwords shared or re-used as passwords on social media sites, a risk potentially compounded if staff discuss their work responsibilities in detail on social media.
- Patients' details discussed in public places or with unauthorised personnel.

Some of these risks were created through good intentions – for example, sharing a smart card with an agency colleague because they couldn't do their job without one. But many were the result of misjudgement. Even those risks that arise for good reasons can and should be engineered out of the system by incentivising staff and improving processes to not work around data security.

The expansion of technology-based data systems in the NHS is reducing the number of risks concerning paper-based information, and can address some risks caused by human error (such as recording of incorrect information). Nevertheless, it has introduced new risks, in particular, exposure to cyber threats as a result of staff receiving emails with potentially dangerous links or attachments, or having unfiltered access to the internet, which have the potential to involve the loss of far larger amounts of data. The threat from cyber attacks has not only put patient information at risk of loss or compromise but also jeopardises access to critical patient record systems by clinicians. This in turn could have a detrimental effect on patient care. This threat is most often introduced from denial of service attacks (attempts to make a machine

*www.ponemon.org/blog/the-human-factor-in-data-protection

or network resource unavailable to its intended users) and ransomware such as 'cryptolocker', but can also arise during the transition between different IT systems.

EXAMPLE

During a previous comprehensive CQC inspection of an NHS foundation trust, we heard that the introduction of a new IT system for clinical records had affected the trust's ability to report, highlight and take action on data collected on the system.

Although the system was beginning to be embedded into practice, it was still having an impact on patient care and relationships with external professionals, and medicines were not always prescribed correctly due to the limitations of the technology.

The risks identified to date are likely to increase as data held by the NHS becomes accessible to many more people, including patients who will soon have access to their own medical records online. The potential for patients accessing their data on insecure devices or through insecure networks, or for their login credentials to be accessed by third parties raises a number of potential concerns about how the NHS can ensure that their data remains secure.

All organisations that provide NHS care are required to comply with the IG Toolkit, but through self-assessment only, so it is very hard to tell whether an organisation is exposed to unnecessary risk. A limited number of areas of the NHS, mainly large dental service providers, are subject to independent validation of data security controls that apply where financial payments are accepted from patients. However, very few NHS organisations are subject to independent external validation of their data security controls. This means that the leaders of most NHS organisations have to rely on internal assurance mechanisms. Yet we found that those too were inconsistently robust across the providers we visited.

1. How well does the organisation's leadership enable staff to keep patient confidential information secure?

KEY FINDINGS

- 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.

Leadership and culture

WHAT GOOD LOOKS LIKE

- Effective leadership is visible and active, and demonstrates clear ownership of data security, just as it does for financial management and accountability.
- Leaders test and understand their organisation's exposure to risk and the ways in which those risks are managed. They regularly seek out independent, external validation of their data security.
- Leaders of small general or dental practices, whose IT is often provided by external contractors, recognise that in outsourcing the supply of IT they have not outsourced their responsibility for data security as well.
- Leaders create and maintain a culture where data security is easier to maintain than not, even for front line staff under the pressures of emergency care. There is a culture where mistakes, near misses, and concerns are raised immediately by staff who are then recognised for helping to make the organisation safer.

Our visits showed us that, in general, data security is spoken of seriously across organisations. There was evident commitment at senior management level to ensure that patient data is kept, used and shared in a secure way.

Yet we found limited evidence of leaders testing their own data security arrangements, and sourcing independent external validation of those arrangements with which to assure themselves and their patients of their exposure to risk. In this respect, leadership was found to be poor, and therefore potentially unsafe.

We also found evidence that appropriate policies and procedures were in place to ensure that this commitment is maintained and monitored and that any problems are identified and resolved. However, this was inconsistent across providers, ranging from a complete absence of such measures, to them being fully embedded.

In hospital trusts and in GP and dental practices that were part of larger organisations, we saw evidence that data security was discussed in staff workshops, clinical handover sessions and ward rounds, IT-led data security audits, through the use of 'secret shoppers', in staff training and surveys.

In most dental and GP practices, the demands of communicating across the service and with staff are less complicated. However, we found a similar commitment to ensuring that data security was treated with importance, and where sites were part of larger organisations (franchised dental practices and grouped GP practices) we generally found them to have structures and systems in place that resembled those in NHS trusts.

Many organisations were proud of having what they described as a culture of openness and honesty about data security and breaches. There was a strong belief that this was beneficial to improving data security and to staff feeling empowered and encouraged to report potential incidents.

We were commonly told that organisations had a culture of 'learning not blaming'. However, we found evidence in these organisations of breaches not being learned from, and junior and contract staff reluctant to challenge what they regarded as unsafe behaviour. For example, cleaning and portering staff were left alone with paper and electronic records, and some told us they had been witness to breaches and potential breaches in data security by those in more senior positions, but did not know how to raise or report their concerns.

While we found that most staff took data security seriously, many did not share the confidence expressed by their senior management that incidents are always investigated, action is always taken and lessons are always cascaded through organisations or implemented effectively.

We also found evidence that, for many leaders, data security was considered the job of the IT department. This was mirrored in some smaller organisations that outsourced the supply of IT equipment and appeared to outsource their responsibility for their own data security alongside it. This is of concern, as it demonstrates a common confusion at a leadership level over who is responsible for ensuring IT security and who is responsible for data security.

Training

WHAT GOOD LOOKS LIKE

- Training is mandatory and regularly refreshed for all staff, including those on temporary and agency contracts. It is tailored to the responsibilities of each staff group so that it is accessible and relevant, and has the greatest impact.
- Staff are trained in how to access and share data remotely, and what they can do safely when in environments that do not easily lend themselves to privacy.
- If staff are ever in doubt about an issue, their training equips them to find reliable guidance quickly and easily.
- Staff recruited to senior positions with significant responsibilities, such as SIROs and Caldicott Guardians, are also properly trained and their training is kept up to date with materials relevant to their roles.

We found a mixed picture in respect of staff training on data security.

In some cases, it was clear that staff only completed training because it was mandatory and not because it was viewed as relevant or likely to be useful. This was revealed in many accounts by staff who reported that training was a 'tick box' activity that was given little status or time.

In other cases training was thorough, appropriate, role-relevant and regularly repeated. However, even in these organisations this was not the case for all staff, especially those in support roles, such as cleaners and porters.

We also found that contractors delivering services on NHS sites often received no training (this included agency clinical staff) and some staff raised concerns that training for external health providers with whom they shared data was either non-existent or insufficient.

It is of particular concern, given their role in leading the delivery of data security, that training for SIROs and Caldicott Guardians was found to be variable and in some cases non-existent. In some organisations, the post holders did not feel they had any status at a management/board level and did not feel they could deliver the role effectively.

There were also instances where the recruitment to these senior roles was too informal. In one case, the individual did not realise that they were the post holder until prompted by their colleagues.

We also found that people in these positions often found it difficult to manage the role alongside their other responsibilities. Worryingly, some said they had little or no awareness of data security and, more specifically, issues relating to IT.

Patient access to their own data

WHAT GOOD LOOKS LIKE

- Patients are well informed about their rights and staff are clear about what information they can and cannot share under different circumstances.
- Patients are advised about how to protect their own data when accessing it online or discussing it in places where confidentiality cannot be assured.

We found that, in most cases, information was readily available to patients and relatives about how they could access information held about them.

Staff were generally aware of what information patients and their relatives were entitled to see, and of the procedures to ensure this was done legally and safely.

There were, however, some examples of confusion with regard to handling patient requests for copies of information held about them (subject access requests). Some staff believed patients can see anything they ask for and others were uncertain how to respond to requests from lawyers, the police and relatives.

There was a range of concerns raised around how to deal with suspected child safeguarding issues – for example, where an estranged parent wanted to remove their child from hospital and the nurse on duty could not find all of the relevant information to support a decision.

By 2018, patients will have electronic access to their own medical records. This raises additional risks about how data can be kept secure once access is shared with the wider population, many of who may not be sufficiently aware of their data security needs and responsibilities.

Without substantial improvements, we cannot assume that the typical causes of accidental breaches existing now will not also be found among new uses of the system – sharing of passwords, accessing data through unencrypted channels and devices and relatives or others accessing and perhaps seeking to change the confidential records of vulnerable patients.

2. How well do the organisation's processes ensure the right levels of security of patient confidential information?

KEY FINDINGS

- 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.

Staff access to patient records

WHAT GOOD LOOKS LIKE

- Access to confidential information is set according to what staff need in order to carry out their duties effectively and safely.
- Access to confidential data is withdrawn when staff move to different duties that do not require the same access, or when they leave the organisation.
- Attempts to log into secure systems are treated with caution and only authorised people gain access.
- Logins to systems are controlled by unique personal usernames and passwords and are changed frequently.
- Where smart cards are used, everyone has their own. Agency and new staff are issued with their own cards as soon as they arrive, and all cards no longer needed are cancelled immediately.

In general, access to data was determined by the specific needs of staff to carry out their roles effectively and safely. In almost all cases, access to IT systems required staff to log in using a personal username and password. In addition, almost all trusts and many GP and dental practices had implemented some form of smartcard access control. However, this approach was not universal and we found many examples where access did not appear to be secured or controlled sufficiently and where there was evidence of potential risks.

Where smartcards and passwords were used, there was a strong belief that these significantly enhanced data security. In some cases, however, the belief that the system was secure meant that individuals did not feel it was so important to be vigilant of data breaches caused by members of staff.

Some managers did not appear to fully recognise the risk when policies and guidance did not align with actual day-to-day practices. We found examples where sites did not have procedures in place to:

- Stop staff being issued with cards with generic access to physical spaces.
- Ensure there were controls over which areas of the network staff could access and make sure these were regularly reviewed and updated.
- Prevent staff sharing cards, user names and passwords.
- Ensure that new and temporary staff were provided with cards/passwords in a timely manner.

We also saw a number of examples where controlled access to secure areas was undermined by staff entering an area with a colleague and not using their card. Similarly, we were told of instances where doors were propped open. This was a commonly reported issue on larger sites.

We did, however, find many examples of good practice on many sites, including:

- Patient files being stored in locked cabinets in secure areas.
- Computer screens in reception areas being positioned so that unauthorised people could not see them.
- Staff not using patients' names or personal details on the telephone and having conversations in private.
- The widespread use of patient 'self check-in' systems.
- The use of secure envelopes for moving patient files.

Mobile and remote working

WHAT GOOD LOOKS LIKE

- Staff are provided with encrypted devices so that they can work safely and effectively anywhere on site, and off site whenever necessary.
- Staff are trained and supported to carry out their work securely without compromising their need to access data when and where needed.

We saw, and were told about, many examples of staff using remote devices such as smartphones, tablets and laptops in ambulance trusts, community trusts and in accident and emergency departments. In dental and GP practices, the use of remote working and mobile technology was much more limited.

We found that a considerable amount of guidance had been provided to staff on the vulnerability of such equipment, especially when being used in public places. This included specific guidance on where and when such devices should be used for accessing and recording patient data, in particular when using public or non-secure Wi-Fi and email. It also included controls and guidance on what type of information staff could access when using virtual private network (VPN) connections.

In almost all cases, mobile devices that were being used were encrypted and used VPN connection from remote sites. However, we did find some examples where unencrypted or unsecure connections were being used or where staff did not know if devices and connections were secure.

Staff raised concerns about the speed and reliability of remote connections along with a lack of access to 'out of hours' IT support. Some noted that this often resulted in staff developing workarounds, including printing records, which introduces further risks.

For providers who rarely had a need for remote access, we found they tended to transport paper records (for example to satellite offices or patients' homes) and would later scan the record and dispose of the paper copy securely. There was a range of protocols in place for moving such records around, including secure envelopes or lockable box files, and for recording where they were located and who had removed them from the normal storage location.

Organisational learning and comparison through benchmarking

WHAT GOOD LOOKS LIKE

- Taking every opportunity to learn and share from others facing similar challenges.
- Comparing performance with others as a way of stimulating innovation and maintaining continual improvement.

The IG Toolkit, which is designed to allow organisations to assess themselves or be assessed against information governance policies and standards, was generally considered to be a useful guide on which to examine data security issues and prioritise areas for improvement and

training. However, it was also considered by some as being out of date, too rigid and unfair in its scoring, with some providers saying that they did not trust others' assessments.

We found little evidence that organisations benchmarked themselves with others in order to learn from and improve their own data security arrangements.

Only a small number of organisations said they knew how they compared to others in relation to their data security arrangements. Similarly, only a few thought that formally benchmarking themselves against other similar organisations was worth doing.

Working with other providers to understand where improvements could be made would help to develop more standardised processes of securely handling data and encourage greater sharing of data safely.

Business continuity

WHAT GOOD LOOKS LIKE

- Recognising and planning for all emergencies. Developing and practising detailed plans that enable services to continue for the needs of patients.

Most organisations had policies and procedures in place to protect and retain access to their data in the event of an emergency. Most backed up their data to off-site facilities, while some used third party companies to do this on their behalf.

In some small dental and general practices, a back-up drive was taken home each night by a senior member of staff or the practice manager. They were trying to strike the right balance between the risks of leaving data on site and carrying it off site for safe keeping. They expressed their own misgivings about which was preferable. In some cases, it was not clear if the data was stored in a secure/encrypted form.

Most providers had detailed plans that set out how they would continue to provide safe services in the event of an emergency (such as fire, theft or other event that would make existing data potentially inaccessible).

Generally, we found clear lines of command and policies in place that covered a range of eventualities. The plans that we reviewed included cancelling patient appointments, transferring patients with urgent needs to other providers, and reverting to paper records.

We found some sites that had no business continuity plans and others where staff could not remember where their plan was stored and had rarely tested it. We also came across examples where plans were unlikely to be effective. One dentist told us that their plan was stored on their shared network drive and had not considered how they would access it if the network became unavailable.

It was common among staff in smaller sites for them to not be aware of any such plans.

3. How well does the organisation equip itself with paper record keeping systems, hardware, software and IT updates to a standard suitable to ensure security of patient confidential information?

KEY FINDINGS

- 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 front line 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.

Control of removable records

WHAT GOOD LOOKS LIKE

- Removable records include paper, USB drives, CDs, DVDs, external hard drives and storage devices, and well-led organisations avoid any of these media being left unlocked and unattended at any time.
- Paper records are kept in locked cabinets, carried securely and not left in public areas. USB ports and CD or DVD drives are all locked away securely.

The effective storage and handling of paper records was mixed. In some GP and dental practices we saw that patient records were locked in secure cabinets away from public access areas. In others they were kept in unlocked filing cabinets in the waiting room.

In general, we found that the trusts we visited stored patients' records safely and securely. However, we had concerns about how they were sometimes transported to different departments in unlocked trolleys, or with no protective cover in the back of patient wheelchairs. We were also told of numerous examples where patient records were left on reception desks without being handed directly to a member of staff.

In most organisations, management was of the view that the policy on the potential security risks of USB drives and other removable storage devices was clear and was communicated effectively to staff. However, particularly in some smaller sites, the extent to which organisations monitored and enforced these policies was mixed. In some cases, managers were of the view that telling staff not to use USB devices or connect mobile phones was sufficient (in most of these sites providers did not permit the use of such devices at all). In larger sites, where we saw poor practice, the policy was considered to be effective but in reality was not always followed, or tested.

Where removable storage devices were used, we found some evidence that USB ports were not locked to prevent data being copied and saved to unauthorised or unencrypted devices.

This lack of active protection also enabled staff in some settings to connect unauthorised mobile phones to a PC, which could potentially introduce a network security risk. We found a similar situation in respect of CD/DVD drives.

Ease and speed of access to data

WHAT GOOD LOOKS LIKE

- Staff have secure access to patient data when and where necessary so that they can effectively treat each patient without delay.

While most organisations had secure practices in place for the use, storage and disposal of all forms of data, this was not always the case. The challenge remains to ensure that the security of systems does not affect the availability of information as this can result in delays to patients' treatment.

While the consequences of data loss or unsafe information sharing are considerable, so too are the consequences of protecting data to a level that it is not accessible when needed. In this regard we found that, in some instances, clinical staff had invented unsecure workarounds to prevent delays to their patients' care.

We found evidence in all types of provider, but most notably in hospital trusts, that systems had not been built around the users' needs, which caused delays for staff trying to obtain vital information quickly, often under emergency conditions.

Many members of staff told us that IT systems cause delays by forcing them to repeatedly sign in and out. This was a particular issue for staff working in areas such as accident and emergency, where speed of access was essential.

In one A&E department, staff had to log in to one system to access information, then log out before moving to another area of the hospital and log in again to continue treating the patient. In this instance, staff were accessing systems using shared passwords to prevent going through the lengthy processes of logging in and out. We were also told that data can be held on multiple, and incompatible, systems requiring multiple sign-ins and in a mix of electronic and paper forms. This was forcing staff to make decisions on the basis of partial information and with uncertainty as to whether more up-to-date information existed.

A senior nurse in a children's ward told us that she often had to make decisions in the early hours about care or safeguarding arrangements, when she either did not have access to all the information she needed or she worried that some information might be available elsewhere in the trust, but could not access it when she needed to.

Data sharing

WHAT GOOD LOOKS LIKE

- Data is shared quickly, effectively and safely with all those involved in the care of patients, including staff in different organisations.
- Staff understand the importance of sharing data and are assured that they can do so safely and securely.
- NHS organisations are supported to work together to agree common arrangements for data sharing.

In some organisations, we found evidence of good data sharing and good data security. This was particularly true where organisations had mechanisms in place to ensure systems used by both senders and recipients in data transactions were trusted.

Despite this, we found that sharing data in and between organisations is something that is commonly viewed as a challenge. Organisations reported difficulties in ensuring that staff always had the right level of access to data without security being compromised.

Many GPs and dentists told us about their inability to access secure hospital systems, including NHSmail (a secure email service approved by the Department of Health for sharing patient identifiable/sensitive information), while some hospitals talked about their concerns that some GPs and dentists were running highly insecure systems (for example, systems with out-of-date support agreements).

In both cases we were told of numerous examples where workarounds to sharing data raised potential data security risks – for example, the use of insecure fax transmissions.

In some instances, we found 'information sharing agreements' between different organisations (such as NHS trusts and other local providers) that clearly outlined key policies and practices. These were often developed in the context of well informed and committed staff who aimed to ensure that information governance and data security were as good as they could be and that all training and information was relevant and up to date.

This issue of committed individuals driving forward good practice was evident in examples of emerging local/geographical networks who were seeking ways to develop data sharing.

EXAMPLE

An NHS trust in London is leading a project to engage people in their own care and enable health and social care professionals to provide care in a more integrated way.

Through an online system, known as the Care Information Exchange, patients will be able to see, add to and share information about their health and care such as appointments, care plans, test results, referral letters, monitoring data, medications, diagnoses and allergies.

The programme is working with health and social care organisations in North West London and has the potential to involve more than 400 GPs from eight CCGs, social care organisations in nine London boroughs, eight acute trusts, two mental health trusts and four community trusts. It is specifically designed to:

- Give people a single point of access to information about their own care that is held by different organisations.
- Allow people to share relevant aspects of that information with health and social care professionals as and when required, and to record and monitor information about their own health and care.
- Provide tools to improve communication between people and health and social care professionals, such as secure messaging and video conferencing.

Only those organisations that have signed an information sharing agreement will be able to participate in the programme. The system sits behind the NHS firewall and data is encrypted so that the only people who can view the data are the patient and those who have been granted access.

IT security

WHAT GOOD LOOKS LIKE

- In safe, well-led organisations, IT systems are supported and maintained so that they are fit for purpose and are tested with the results being formally and regularly shared with the organisation's leadership.
- Data security arrangements are designed around the needs of patient care and the responsibilities of front line staff.
- Plans are developed to maintain data security and effective access while supporting closer integration of health and social care.

The 2014 IT Health Check Strategic Data Assurance Report for the Health and Social Care Information Centre (HSCIC) has been used to understand the technical aspects of data security in the NHS. The fieldwork we carried out for this review complemented this report by asking how organisations procured, managed, monitored and reviewed their IT infrastructure and software. We also asked how this worked in practice in the day-to-day delivery of patient care.

We found a mixed picture, and one that raised concerns about how data security was approached in all organisations in the context of the way in which IT infrastructure is designed, procured and secured.

As might be expected, we found that large organisations had dedicated IT departments and were often able to devote significant resources to manage complex IT arrangements in-house. We also found several examples where investment had not been made and so appropriate equipment was not in place, and in-house capacity and capability were poor.

Smaller organisations more commonly outsourced their IT provision and support to specialist third-party organisations. Some GPs and dental practices procured all aspects of their IT provision and support through clinical commissioning groups (CCGs) and commissioning support units (CSUs).

While the set-up in respect of different organisations varied considerably, we found that staff in larger providers were often of the view that the junction between IT matters and data security were the responsibility of the IT department. We also found that smaller providers who had outsourced their IT needs often appeared to think that this meant they had effectively outsourced their responsibility for security. This was evident in many review visits, when management expressed concern that they simply did not know about aspects of the IT procurement and such specifics as whether their data was backed up securely and how they could access it if they needed to.

In both cases, we found that staff (including management) often did not seek assurances as to how equipment was configured to provide appropriate levels of control, whether back-up data was encrypted or accessible or whether/how network monitoring was being conducted. Where such assurances were sought, we still found these to be limited.

EXAMPLE

One trust believed it had robust IT security processes until it fell victim to a cyber incident that resulted in its server being used to send out spam email.

Emails were being digitally signed by the trust indicating that the hospital's email had been hacked as a way to avoid spam filters.

The trust reported the cyber security incident and alerted the ICO, HSCIC, NHS England and its commissioners. In addition the incident was formally reported to the police as a potential criminal matter.

A response team was employed to monitor the situation, to make informed decisions and take any necessary immediate actions. The trust also commissioned cyber security expertise and received the following recommendations to:

- Implement best practice in management of its firewalls, network and servers.
- Ensure anti-virus software is continually updated.
- Review the allocation of responsibility for each server and IT system.
- Make sure staff are aware of the risks of cyber attacks and know how to respond should there be further incidents.

The trust is working on an improvement programme that will include regular routine testing of its data security systems.

It appears that, in many circumstances, there is an over-reliance on policies and procedures rather than testing that systems are sufficiently secure. There is often little focus on implementing procedures to monitor and enforce the policies that are in place. This lack of assurance reinforces the fact that however secure a new IT system might be, it can only ever ensure data security when systems are used correctly and policies are enforced, internally audited and externally validated.

Some examples of the potential data security issues that we encountered include: staff being able to use networked devices for unfiltered internet browsing; being unclear how to respond to links in external emails; potential spam or phishing attempts; and inadvertently introducing viruses to the network.

These examples indicate that the often interchangeable use of 'confidentiality', 'data security' and 'information governance' means there is a risk that staff can make the wrong decisions about how to protect and share patient data. For example, a patient's medical history needs to be kept secure when sharing it with another provider involved in their care, but if it is also kept confidential, vital information could be missed. Keeping data secure is vital for good care, but keeping it confidential from those who need to know it puts effective care at risk.

Recommendations

We were asked by the Secretary of State for Health to make recommendations on:

- How current arrangements for ensuring NHS providers protect personal data could be improved.
- How the new guidelines (published by the National Data Guardian, Dame Fiona Caldicott) can be assured through CQC inspections, NHS England commissioning processes, and any other potential mechanisms.

Paper records account for the great majority of data breaches reported to the Information Commissioner's Office. However, the Government has said that all patient records must be held electronically by 2020, so it can be assumed that this particular risk will eventually be removed. In the meantime, risks related to paper records must continue to be addressed.

Unless current arrangements for the security of all other data are improved, the risks that currently exist will be magnified when information held by the NHS is made more accessible to the public. Consideration must be given to safeguarding patients' access to their own records so that they do not mirror the insecure behaviour identified in this review.

Data security should never be used as an excuse not to share data that meets the health needs and expectations of patients. Sharing data enables patients to receive effective care in a timely manner. Guidance on data security needs to be improved to ensure people have a detailed and relevant understanding of issues around confidentiality and consent, and of how data will be used in the delivery of care.

We are clear that responsibility for data security sits with providers. Discharging this responsibility requires visible leadership that establishes a strong culture, one that recognises the importance of data security and supports staff to use information effectively to provide patient care. In addition, it includes putting in place the appropriate assurance processes that satisfy them and others that systems are effectively implemented and monitored.

As set out in this report, our main areas of concern relate to leadership, behaviours and systems.

The leadership in a large NHS trust includes a chief executive and a board of directors. In smaller primary care settings the leadership may only include a senior partner. The responsibilities in both are the same, though the extent of the task will differ according to the size and complexity of the organisation.

Our recommendations seek to improve current practice without imposing unreasonable extra cost on healthcare providers. Investment of time and money should be considered against the relative level of risk to data corruption, availability of data, the potential consequences to patient care and the financial expense of data recovery.

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.

The effectiveness of their organisation's data security arrangements should be tested and internally audited to understand their true exposure to current and known future risks, including in instances where IT is outsourced to third party providers.

They should secure external audit or other validation of their internal assurance processes and set objectives for improvement of data security arrangements.

In practice, this means that senior leaders should:

- Include data security on their organisation's risk register and regularly review progress against objectives.
- Compare their data security performance with those of other organisations and commit to sharing with, and learning from, others.
- Assure themselves that data is made available safely to those who need it for patient care when and where they need it, including in other organisations.
- Assure themselves that data security arrangements are designed around the needs of patients and the care given by front line staff.
- Assure themselves that their organisation is making effective arrangements for all emergencies, and developing and practising detailed plans that enable services to continue for the needs of patients in the event of a major data security breach.
- Establish an organisational culture of learning, not blaming, in relation to data security. They should include proactive encouragement of incident reporting where learning is identified and shared as part of ongoing training and awareness raising. Formal mechanisms should be put in place to ensure this happens and that all staff are aware of what improvements have been made as a result.
- Have named senior responsibility and accountability for all aspects of data security – including confidentiality, integrity and availability of data – to ensure it is taken seriously and acted on.
- Provide staff who are responsible for data security with access to relevant support from NHS England, CCGs, CSUs and HSCIC to enable them to deliver their responsibilities.

Recommendation 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.

In practice, this means:

- Data security training is improved by being made mandatory for all staff (including agency and temporary staff, is role-specific, including how to work safely remotely on encrypted devices) and is regularly updated.
- Responsibility for training sits with a named senior manager, and is developed with input from staff to ensure it covers relevant scenarios and provides them with clarity on the right courses of action.
- Specific clear guidance is provided to all staff on how to raise concerns and how to report actual and near incidents and data breaches. This will be done as part of the development of a culture in which staff are empowered to raise concerns and report incidents.
- Support is provided by NHS England and HSCIC to ensure that rapid progress can be made simply and cost effectively. HSCIC will also work with, and point to, external providers of support, training and auditing.
- Arrangements to keep removable records readily secure and accessible are reviewed and improved (for example, in lockable USB ports and drives and paper filing cabinets).
- Through its planned refresh by HSCIC, the IG Toolkit will be re-developed to recognise the characteristics and needs of different types, sizes and maturity of providers, and provide more tailored support. It will provide assurance and knowledge of vulnerabilities, and become a portal through which support can be accessed.
- Using the refreshed IG Toolkit, HSCIC and NHS England will actively look for providers that they view as high risk (or who report having a concern themselves) and provide them with support as a matter of priority. Different providers need different support and could be assisted through identified local buddying and good practice benchmarking.
- Common procedures on data sharing across local and regional health providers would be developed. This would enable providers and commissioners in the same locality to work closely together and streamline the currently very different arrangements providers have with one another.
- Revised information would be provided to patients on how their data is shared between relevant NHS staff and organisations involved in their care and additionally set out their responsibilities in protecting their own data.
- Robust mechanisms for recruitment and training of SIROs and Caldicott Guardians, and clarity of accountability for all aspects of data security would be ensured.

Recommendation 3

IT systems and all data security protocols should be designed around the needs of patient care and front line staff to remove the need for workarounds, which in turn introduce risks into the system.

Data security comprises confidentiality, integrity and availability. If data is not available when needed by those in front line roles, then however confidential the data might remain, it cannot be said to be enabling good quality of care.

In practice, this means:

- All organisations would carry out a comprehensive review of their current systems and protocols for handling patient data, including electronic and paper records. This would inform a strategy to simplify and clarify the systems that are currently in place, identify redundancies and incompatibilities and eliminate, as far as possible, the use of multiple systems. This process would be continued as part of all organisations' strategic planning and ongoing management processes.
- When proposals are made to introduce any new systems or replace existing systems, staff will be involved in planning from the beginning to ensure transition, accessibility and usability.
- Organisations would document how the transition between old and new systems will be managed. This would include the process for data to be made available on a replacement system, a clear plan for how the transition from current mixed systems of IT and paper-based data will be managed, and how any business continuity plans will deal with any reversion to use of paper records while these remain in use.
- All aspects of procurement (equipment, software, support and training) would meet a common standard as specified by NHS England and HSCIC. This would be incorporated into contracts for all providers/suppliers from NHS England to third party providers and individual sites (for example, ensuring unsupported software and insecure browsers are removed and anti-virus/firewalls are in place) and would have specific plans in respect of mobile technology and remote and agile working, ensuring all devices are encrypted.

Recommendation 4

Computer hardware and software that can no longer be supported should be replaced as a matter of urgency.

In practice, this means:

- NHS England and HSCIC would set a date beyond which out-of-date and unsupported systems are to be no longer used.
- This requirement would become part of all standard contracts with third party providers.

Recommendation 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.

In practice, this means:

- The new data security standards under development by the National Data Guardian would be implemented by organisations whose leadership can then assure themselves of their own compliance.
- As set out in Recommendation 1, the leadership of provider organisations would secure external audit and validation of their internal assurance from a number of bodies, including HSCIC and audit providers.
- HSCIC will assist provider bodies by giving advice and helping with peer to peer learning and encourage stronger performers to work alongside those with more improvements to make.
- The Department of Health, NHS England and HSCIC will consider making existing tools for assuring data security, including the IG Toolkit, externally audited or validated, to improve on the current reliance on self-assessment alone.
- NHS England and CCGs would re-consider contracts with providers who, after a reasonable period, do not meet the new commitments, fail to secure external validation of their data security arrangements, and therefore continue to present risks to their patients and other providers.
- CQC will work closely with HSCIC to explore potential links between the issues of data governance and security, and the quality of care.

Recommendation 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.

In practice, this means:

- CQC will strengthen its existing key lines of enquiry on information governance.
- CQC will make use of external audit or validation results in its future assessments, as it does for other highly specialised topics audited by others.
- HSCIC will inform CQC of provider bodies with repeated breaches, so that any need for follow-up can be appropriately determined.

Care Quality Commission

How to contact us

Call us on › 03000 616161

Email us at › enquiries@cqc.org.uk

Look at our website › www.cqc.org.uk

Write to us at ›
Care Quality Commission
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4PA

Follow us on Twitter › @CareQualityComm

Please contact us if you need a summary of this report in another language or format.

CQC–304–072016