CareQuality
Commission

Policy statement on information security and governance

July 2016

The Care Quality Commission is the independent regulator of health and adult social care in England. We make sure that 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 health and adult social care providers.
- We monitor and inspect services to see whether they are safe, effective, caring, responsive and well-led, and we publish what we find, including quality ratings.
- We use our legal powers to take action where we identify poor care.
- We speak independently, publishing regional and national views of the major quality issues in health and social care, and encouraging improvement by highlighting good practice.

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

1. Introduction

Having timely access to information and using valid, robust, and relevant data securely underpins both the provision of good quality care and the efficiency and effectiveness of all organisations involved in the health and social care system in England. This policy statement sets out how CQC carries out its regulatory role with regard to the secure use of information by health and adult social care providers, and how we securely handle data ourselves in line with expected standards.

The policy statement also provides a response to the recommendations from the National Information Governance Committee, which gave independent and objective advice on development and delivery of CQC's information governance monitoring functions. We have accepted these recommendations and will continue to identify how we can strengthen the use of information in our future regulatory approach. Appendix B of this policy sets out the recommendations and our response in more detail.

The Health and Social Care Act 2012 gave CQC new legal responsibilities from 1 April 2013 to enable us to monitor and seek to improve the information governance practices of registered providers. The Act did not give CQC any new powers in relation to these functions, but CQC was required to set up a National Information Governance Committee (NIGC) in June 2013 to provide advice on developing and delivering the new responsibilities.

The NIGC provided advice and support to CQC to develop a confident and meaningful approach to monitoring information practices among registered health and adult social care organisations. It also identified areas for learning and improvement in the way that information is used to support good quality care for all people who use health and social care services and to share these appropriately. The NIGC submitted its recommendations to CQC's Board in July 2015.

In late 2015, CQC carried out a thematic review to establish whether personal health and care information is being used safely and is appropriately protected in the NHS. The report of the review, *Safe data, safe care*, was published in July 2016. It sets out recommendations that have informed our future plans – both for inspecting information governance by providers and for our own approach to data security.

Why information security matters for quality

Information security includes all forms of information – paper-based records, electronic documents, electronic data, x-ray and other images held electronically and physically, sound recordings and the spoken word.

CQC is part of a large and varied group of organisations that are active in the field of information security and governance, including data handling, data use, data sharing, and data security. Each organisation has different remits and powers (see appendix A).

As society changes and people live longer with multiple or long-term conditions, having access to individuals' personal information and sharing it securely and in real time across different providers is central to well-designed, joined-up, and properly co-ordinated care. This benefits the person using a service, as it ensures that their care is centred on their needs, removes the need for them to repeat their care 'story' many times to different clinicians, and allows a seamless transition between different health and care providers. It also enables individuals to take more control of their information and can support them to self-manage their care.

For providers of care, using information properly creates an opportunity to work more efficiently and effectively with local partners to develop a fuller picture of individual care needs, and needs across a local area, on which to plan efficient and effective services for the future. Done well, using the same information for multiple purposes reduces the information burden across organisations within the system by collecting what is needed, sharing it appropriately, and maintaining a clear, shared focus on people's health and care outcomes.

The fast growth of technology means that there are digital applications on the market aimed at helping the public to understand or monitor many aspects of their lives. This has resulted in a greater public appetite for accessing health and care services in the same way. By 2032, everyone is expected to have access to the internet everywhere, which means there will be opportunities to capture, relay and interpret information in our homes, hospital or care setting.[1] For example, video conferencing and other remote services may well become mainstream activities in some sectors.

The growing number of lifestyle apps that enable personal health data to be captured and shared across online communities and social media means that the health and care sectors need to do far more to secure patient data. They also need to make it much more accessible to individual patients and different care providers. This will be challenging for all organisations.

We therefore need to understand how to ensure that people's records and information are shared securely between services, and can be used to promote better quality care.

Confidentiality, security, and data sharing are not contradictory requirements – the evidence from CQC's data security review suggested that those organisations that were confident in their data security arrangements were also most confident about sharing data speedily. Both are essential ingredients for high-quality care.

[1] Imison C, *Future Trends: An overview*, Kings Fund, p6 (November 2012).

2. CQC's guiding principles on information security and governance

High-quality care will only be achieved when robust information is available, shared, and used effectively and securely. CQC is also in a unique position in the health and care sector to encourage improvement by making greater use of our analyses of the regulatory information that we gather.

To do this, we need the public, providers and partners to have confidence in the data that we collect and in how we manage our information systems. We are committed to the following three principles that we believe are essential for all organisations in health and social care:

Availability*:* Data must be available when and where it is needed. It must be made accessible swiftly and securely for staff as well as within and between organisations.

Integrity: The data must be valid and trustworthy, relevant, up to date, and protected from loss, damage, and unauthorised alteration.

Confidentiality: Personal identifiable data must be handled and used safely.

To enable us to implement the above principles, it is important that:

a) We consider good information, handled and used in line with these principles, to be an integral part of good quality care.

b) We are part of the health and social care system, and as such, we want to adhere to the same expectations that we have of providers, and be a role model for the way we handle and share information ourselves.

c) We work together with national and local organisations to ensure that our approach is aligned with their respective areas of work and responsibilities.

d) We work more efficiently and effectively with other regulators and partners to minimise the burden on providers through better information sharing, while supporting our ability to perform our regulatory duties.

3. How CQC currently regulates providers' information governance and use of data for improving the quality of care

CQC's overall operating model for the regulation of health and adult social care is based on registering, monitoring, inspecting and rating providers. We also take enforcement action and provide an independent voice on the quality of care in England.

To support our operating model, our inspection teams use a standard set of key lines of enquiry (KLOEs) that directly relate to the five key questions we ask of all services: are they safe, effective, caring, responsive and well-led?

Registering care providers

Any person (individual, partnership or organisation) who provides a regulated activity in England must be registered with CQC by law. We register services against fundamental standards and other relevant regulations, which include information governance and data security.

At the beginning of the regulatory process, we consider whether organisations have systems and processes in place to collect information that is relevant to the care of people using their services, and how they store and manage information effectively so that people's personal data is secure. As part of the registration assessment, new providers must demonstrate their understanding of information governance and how to use data effectively and appropriately (see www.cqc.org.uk/providers-how-we-regulate). Appendix C sets out the regulations that support information governance and use of data.

Before we grant registration, we assess all applicants to ensure that we are satisfied about their fitness and compliance with the requirements of the relevant regulations. Our assessment may include a site visit.

Figure 1: Focus areas for registration assessments covering information governance and use of data in the effective, caring and well-led key questions

Effective

- Ensuring that relevant and appropriate information about people's care and treatment can be shared between other providers and services when people are admitted, transferred or discharged.
- Sharing and coordinating information with other providers and/or services in an emergency.

Caring

- Providing appropriate information to support and enable people to make informed decisions about managing their care and treatment.

Well-led

- Systems for reporting and learning from incidents.
- Systems to maintain secure, accurate, complete and detailed records for each person using the services and records relating to the employment of staff and the overall management of the regulated activity.
- Governance systems for scrutiny and overall responsibility at board level or equivalent.
- Assurance that records about staff employed and the management of regulated activities are created, amended, stored and destroyed in accordance with current legislation and guidance.
- Robust arrangements to make sure that information sharing systems comply with the Data Protection Act 1998.

Monitoring, inspecting, rating care providers

Our current inspection framework includes questions about information governance – the means by which information security is overseen. There are now mandatory key lines of enquiry and supporting prompts under the effectiveness key question for the inspection of hospitals (which include acute care, community health services and mental health services) and primary medical services.

Figure 2: Key line of enquiry and prompts for effectiveness in acute trusts, primary medical services and specialist mental health services

- **Effective (KLOE E5): Do staff have all the information they need to deliver effective care and treatment to people who use services?**
  - Is all the information needed to deliver effective care and treatment available to relevant staff in a timely and accessible way? (This includes test and imaging results, care and risk assessments, care plans and case notes.)
  - When people move between teams and services, including at referral, discharge, transfer and transition, is all the information needed for on-going care shared appropriately, in a timely way and in line with relevant protocols?
  - How well do the systems that manage information about people who use services support staff to deliver effective care and treatment? (This includes coordination between different electronic and paper-based systems and appropriate access for staff to records.)

Inspections of adult social care providers look across the three key questions of caring, effectiveness and well-led to gather an overarching picture of information governance and use of data.

Figure 3: Mandatory key lines of enquiry and prompts relating to information governance in adult social care

- **Caring (KLOE C2): How is people's privacy and dignity respected and promoted?**
  - How are people assured that information about them is treated confidentially and respected by staff?
- **Effective (KLOE E3): Is consent to care and treatment always sought in line with legislation and guidance?**
  - How does the service monitor and improve the way staff seek people's consent to their care and treatment to make sure it is acting within legislation?
- **Well-led (KLOE W3): How does the service deliver high quality care?**

  There are two key prompts under this key question:
  - Are quality assurance and (where appropriate) governance and clinical governance systems effective, and are they used to drive continuous improvement?
  - How does the service make sure they have robust records and data management systems?

As part of our role in monitoring the quality of a provider's service in relation to information governance and security, we ask them for evidence of their assurance of completeness and accuracy of information. If this information raises any concerns, or if other concerns are raised with us, we will follow it up with the provider during the inspection process.

In addition, we have specific information sharing agreements in place with a number of organisations, including professional regulators, the Health and Safety Executive and the Coroners' Society, to ensure that we routinely receive certain types of information from them. The data they provide can help us to monitor quality of care. These also include defined arrangements for passing information of concern to us.

Enforcement

We receive information on risks in health and care services from a variety of sources, which can lead to us taking enforcement action where minimum expectations of quality aren't met. This includes good governance of information (see appendix C). Our enforcement decision process includes consideration of whether CQC is best placed to take action, or if we should refer the matter to another body such as the Health and Safety Executive or the police.

When we use all but our lowest level enforcement powers, we always notify interested parties. These include NHS and local authority commissioners, Monitor and the NHS Trust Development Authority and, where appropriate, other providers or services that may be affected. See www.cqc.org.uk/enforcement.

The Information Commissioners Office (ICO) also takes appropriate action on data breaches reported to it, which includes breaches arising from health and social care providers.

CQC's independent voice

We have a statutory responsibility to encourage improvement. This means that we do not only inspect and rate the quality of care in health and social care providers, but we also encourage improvement in the wider sector by using our evidence and information through our independent voice.

For example, our review of transition arrangements from children's to adult services for young people with complex health needs[2] found that they regularly had to repeat their medical history to different healthcare professionals in different services and even within the same organisation. This highlighted a need for better information sharing between staff providing care. Similarly, our review of the journey of care for people with dementia[3] found that the transitions between care homes and hospitals were the times when people were most likely to experience poor care due to a lack of appropriate and timely information sharing. Our review of complaints handling[4] found poor use of information from feedback with which to improve services.

The findings from thematic reviews have informed how we inspect providers' information governance processes and the extent to which they use data well to deliver high quality and person-centred care.

The Quality of Care in a Place pilot project explored how CQC can comment on the quality of care in a geographical area, beyond what we have observed within individual providers. Within the assessment framework for North Lincolnshire, we asked what role data had in enabling high-quality care in the area – both from a population and whole system perspective. The Quality in a Place reports were published earlier this year. See www.cqc.org.uk/qualityinaplace.

Our review of data security arrangements in NHS organisations, *Safe data, safe care*, identified several issues of concern that related to the safe and effective sharing and use of data, both within and between providers of health and social care.

[2] Care Quality Commission, *From the pond into the sea: children's transition to adult health services* (June 2014).
[3] Care Quality Commission, *Cracks in the pathway* (October 2014).
[4] Care Quality Commission, *Complaints matter* (December 2014).

What we will do

Making data available when and where it is needed will be an increasingly important feature of safe, effective care in well-led organisations.

CQC will therefore amend its assessment framework and approach to inspection to include checking whether providers have ensured appropriate internal and external validation against the standards being developed by the National Data Guardian. We will make sure that CQC inspectors who are involved in this are appropriately trained, as recommended in CQC's report *Safe data, safe care* (recommendation 6).

As part of evolving our approach on future inspections, we will consider whether providers in all sectors are working collaboratively, and consideration of this must include how effectively they share and use information.

We will describe what good looks like in relation to how health and social care providers use and share information, and refer to this in our inspection reports and thematic reviews.

By doing this, we will improve our own processes to look at good use and management of information, as recommended by the National Information Governance Committee.

To deliver this, we will:

a) Offer advice and assistance to HSCIC on improving its support to providers.

b) Strengthen our assessment of how well providers test and assure their own data security arrangements following the recommendation made in our data security review, *Safe data, safe care*, which will involve:

- Reviewing KLOEs and prompts on information and information security.
- Expecting providers to have internally audited their performance where appropriate, and to have secured external validation of the quality of their arrangements; we will use the findings from those exercises to inform our inspections.
- Identifying and using information from HSCIC and other partners about the providers that may have the most risk to enable us to carry out more focused inspections, in line with CQC's next phase of regulation.

c) Further develop and test our draft Information Governance Inspection tool in 2016 as part our strategy for 2016-2021.

d) Update training for our inspectors as appropriate.

e) Develop information governance knowledge and data security expertise in a small group of staff (for example, inspectors and specialist advisors) as part of the next phase of inspection.

f) Include information on how providers use and share data, and how they ensure its security, in our State of Care report and annual report.

4. How CQC's own data is secured and used in line with data standards

In *Safe data, safe care*, our review of whether personal health and care information is being used safely and is appropriately protected in the NHS, we made recommendations for health and care services to improve. Five of our six recommendations made to these organisations apply equally to CQC.

The recommendations urge the leaders of every organisation to demonstrate clear ownership and responsibility for data security in the same way that they do for clinical and financial accountability. This involves testing and internally auditing their own organisation's data security arrangements to understand current and future risks, including where IT is outsourced to third party providers. The report also recommends securing external audit or other validation of internal assurance processes and setting objectives to improve data security arrangements. Both internal audit and external validation needs to be reviewed and strengthened to the same level as those that assure financial integrity and accountability.

The recommendations also say that all staff should have the right information, tools, training and support to allow them to work effectively while still meeting 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 front line staff, to remove the need for staff to create workarounds, which in turn introduce risks into the system. Organisations are also urged to replace computer hardware and software that can no longer be supported as a matter of urgency.

Our response to the review's recommendations

We have considered our own approach to data security in the context of our data security review and the resulting recommendations.

Our arrangements provide safeguards for personal identifiable data, financial information, commercially sensitive data (market oversights function), all employee information, and intelligence shared with us by others, complaints, feedback, and all other information that we handle.

Secure data is integral to the work of CQC and we must demonstrate outstanding performance in this area to lead by example. As a public body, it is vital that providers and our partners have confidence in our data and the data we share with them as part of our regulatory activity.

People who use services also want to be confident that we are inspecting and rating health and care services with reliable data to enable them to make informed choices for themselves, and their family and friends.

CQC's information security framework is based on the international standard ISO 27001: 2013 Information Technology Security Management. Our compliance against its requirements are reviewed, maintained and assured regularly.

Our Information Security and Governance policy follows this standard very closely and specifies the baseline controls expected and encouraged within CQC. This is focused on the following areas:

- Infrastructure and IT security
- Security education and awareness training
- Risk management
- Compliance with legislation
- Operational security advice and assistance to the business.

Infrastructure and IT security

This area of work is primarily focused on the data centres that are managed under contract by Atos and Computacenter. Both companies' data centres are accredited to ISO 27001; these accreditations are regularly maintained and checked.

We have also carried out our own review of our suppliers' facilities and found them to be compliant with our internal standards and requirements.

Detailed IT security arrangements are jointly managed through the open service contract by CQC, the Department of Health and NHS England as the primary users of the service.

A joint security group meets monthly to manage and maintain IT security across the service. That meeting also co-ordinates and oversees technical assurance and testing of the infrastructure, including annual penetration testing by specialist third party providers.

CQC services and applications that are external to open service are subject to separate technical tests (penetration tests) and privacy impact assessments to ensure that they also comply with our internal standards and do not introduce security risks.

Physical security arrangements are reviewed at each of our regional offices to ensure that they are robust and protect against unauthorised entry to CQC's facilities.

Security education and awareness training

It is widely recognised that the largest single area of risk of data security breaches for any large organisation is with staff who may make mistakes through a lack of awareness – such as activating links in bogus or malicious emails or simply misplacing and losing sensitive information.

To mitigate this risk within CQC, a programme of regular training and awareness is in place. The primary element of this is mandatory for all staff, and they cannot access shared drives until they have completed this training. The initial training is then backed up by regular awareness reminders published on the intranet under ‘Security Matters’ and announcements alerting staff to specific issues and risks.

A desktop security package is also deployed on all laptops and PCs in use by staff in CQC. This provides additional protection against unauthorised software being executed if a user receives and unknowingly activates malicious links or attachments in unsolicited emails. Issued iPads have an application installed which is ‘Good for Enterprise’ and is widely considered to be secure for mail and access to CQC systems.

Governance and the management of risk

Information risk management is regularly addressed at the internal information governance meetings, where any significant risks and associated mitigating actions are discussed and reviewed.

The Executive Director of Strategy and Intelligence is our Senior Information Risk Owner (SIRO), and Professor Sir Mike Richards, Chief Inspector of Hospitals, is our Caldicott Guardian.

Compliance with legislation

CQC is required to comply with a range of legal requirements that relate to information security. The primary requirement in relation to personal data (information about identifiable people) is the Data Protection Act 1998. These legal requirements are built into the ISO 27001 standards that CQC works to, and are also assessed when developing our internal policies, processes and procedures. This includes reporting to the Information Commissioners Office when we experience any data breaches.

To manage this effectively, CQC has a central point of contact for staff to access advice and assistance about security. This is regularly used to deal with queries on specific issues and problems to help them process information correctly and avoid data breaches.

Section 80 of the Health and Social Care Act 2008 requires CQC to publish a code of practice in respect of the practice we follow in relation to how we will obtain, handle, use and disclose confidential personal information. We are required to keep this Code under review and have revised some of the content to take into account changes in some aspects of the law and to make the Code clearer about how we obtain, use, disclose and handle confidential personal information.

Assurance

As well as compliance with our own internal policy, over the past three years we have been regularly audited internally and externally, mirroring the recommendations made in our recent data security review.

Where data breaches occur at CQC, we assess and categorise them and subsequently report them in line with both ICO and HSCIC Information Governance Toolkit requirements. The external assessments of CQC's arrangements have been carried out by the ICO and CQC's internal audit and health group, each of which have given CQC a rating of moderate or substantial assurance. The findings from each of these audits have been followed up with action plans and completed in line with the recommendations.

Additionally, we have carried out an internal assessment against the guidelines issued by the Government in 10 Steps to Cyber Security. The result of the assessment was that CQC complies with best practice detailed in the guidance.

What we will do

CQC will continue to lead by example and aim to perform at the highest level.

We will contribute learning and experience to the wider health and care system through membership of National Information Board, and as a partner of HSCIC, and the National Data Guardian. We will follow the recommendations we have made in our data security review and help to shape new standards and system improvements where developed by others and work to ensure that they are designed with the needs of patients and people who use care services in mind.

To do this, we will:

a) Continue to test our own data security internally and secure external validation, with the findings reported to the Board.

b) Comply with all new mandatory standards as they emerge.

c) Comply with the new data security standards being drafted by the National Data Guardian.

d) Review the training offered to our staff, and ensure it is role-specific and supports them to reach the best possible decisions.

e) Share our experience and learning with commissioners, providers, and partners to build collective capability.

5. Next steps

The changing landscape of health and social care means there will be a greater need for person-centred care that is truly joined up and coordinated within and across different organisations. This requires better use of technology and more intelligence-driven systems that can use and share information effectively and safely with other professionals and services, people who use services, and the public.

Information therefore needs to be relevant, useful and timely to make effective decisions about the care of individual people, as well as to prompt good practice in the sectors.

As we implement CQC’s strategy for 2016 to 2021 and the next phase of our inspection programme, we will continue to work with other national bodies and our other local and national partners on using information and datasets securely in a more open and collaborative way. This will encourage improvement in the health and care system by ensuring that information is readily accessible and available to all.

Appendix A: Partners in the health and care system concerned with information and data

Organisation	Role in relation to information and data
Department of Health	Develop and maintain information governance assurance framework for health and social care, including the National Information Board.
NHS England	Statutory duty to publish guidance for registered persons on the processing of patient and other information. Coordinates guidance and standards on using NHS data. Coordinates collaborative working through the Information Services Commissioning Group. Provides strategic leadership through programmes, changing commissioning care and innovations in care (such as the Five Year Forward Vision). May direct the HSCIC to collect patient data subject to the requirements of the law.
Health and Social Care Information Centre	Publishes Code of Practice on Confidential Information. Provides other advice and guidance on data collection and use. Maintains and oversees the Information Governance Toolkit.
Information Commissioner's Office	Independent regulator of the Data Protection Act and the Freedom of Information Act. Carries out data processing audits of public bodies. Publishes guidance on data sharing within the terms of existing legislation.
National Data Guardian for health and social care	The National Data Guardian (NDG) advises and challenges the health and care system to help ensure that citizens' confidential information is safeguarded securely and used properly.
Health Research Authority	Approvals role regarding access to confidential patient information for health research purposes under S(251) through its Confidentiality Advisory Group.
NHS Improvement	An area that is currently under review following the integration of Monitor and the Trust Development Authority. Previously Monitor's role was to enable integration and co-operation between services, while the Trust Development Authority sought assurance of information governance and risk in NHS trusts as part of its accountability framework.
Social Care Institute for Excellence	Provides information, guidance and share good practice.
Association of Directors of Adult Social Services	Accreditation system for research and similar projects.
Local Government Association	Supports its members through benchmarking data service, sharing good practice and innovation. Has an agreed work programme to develop a sector-led approach to data transparency, putting local authority data into the public realm.

Appendix B: Recommendations from the National Information Governance Committee

The Health and Social Care Act 2012 gave CQC new legal responsibilities from 1 April 2013 for monitoring and seeking to improve the information governance practices of registered providers.

It did not give CQC any new powers in relation to these functions. CQC was required to set up a National Information Governance Committee (NIGC) to provide this advice, which was established in June 2013 and ran until October 2015.

The role of the NIGC was to provide independent and objective advice on development and delivery of CQC's information governance monitoring functions.

Recommendation	Our response
1. We recommend that the CQC should ask providers to learn from the evidence of inspections. In particular we urge providers that failed to uphold the highest standards of information governance to learn from the good practice of others.	• **We reported on the importance of good information governance in CQC's 2014/15 State of Care report.** • **Information from inspections and other sources provides insight about providers' information governance systems, and we will monitor this to find good practice.** • **The next phase of inspections will consider information governance and we will highlight and share examples of good practice that we find.**
2. We recommend that the CQC Board completes the task of implementing all the recommendations in the NIGC interim report. They are: Three recommendations for immediate improvements to the inspection system: 2.1 We urge the CQC Board to introduce a mandatory element to ensure that questions about the role of information and information governance in supporting good quality care are asked by inspectors on every inspection and assessed without fail. It is our understanding that the most certain and appropriate way of achieving this would be to include specific examination of the role of information and information governance in supporting good quality care at the level of a Key Line of Enquiry, rather than prompts. Such an outcome would recognise the importance of information in determining whether providers are succeeding in any of the five domains of inspection. Without the	• **This document (to which this is an appendix) also serves as a proposal to fulfil Recommendation 2.** **2.1 Information governance is included in the current set of key lines of enquiry (KLOEs) for inspectors in both registration and inspection – these are mandatory and included in the acute, mental health, and primary medical services handbooks: E5, adult social care handbook: C3, E2, and W3.)** **2.1 We have drafted an information governance inspection tool and will further develop and test this in 2016 as part our strategy 2016-2021.**

right information health and care staff cannot deliver safe and effective care to people who use services and equally services and organisations cannot know if they are providing good care. Without proper information governance, the organisation and staff cannot know whether the information itself is good and tells an accurate picture. The Committee acknowledges and welcomes the fact that the CQC Executive Team has already given consideration to strengthening this aspect of the assessment framework. The NIGC recognises that introducing a mandatory element in inspections has implications for the make-up and training of inspection teams. The introduction of a specific KLOE in at least one domain should be supported by appropriate prompts in other domains.	
2.2 Having made the role of care and treatment information a mandatory part of the inspection framework, it will also be important to ensure that inspectors use this evidence to draw relevant conclusions in inspection reports. To discharge its responsibility to monitor information governance, the CQC must not only ask the questions; it must also capture the answers. The NIGC therefore recommends a clear closure procedure for reporting on the IG KLOE and IG-relevant prompts.	**2.2 We will revise our assessment framework and approach to inspection so that it includes looking at whether providers have carried out appropriate internal audit and external validation against the new Data Security standard.** **2.2 We are also improving our overall evidence collection and reporting processes from key lines of enquiries to final report as part of evolving our inspection approach.**
2.3 The NIGC agree that capacity and capability throughout the inspection process is crucial. There should be information and IG capability within the inspection teams themselves. The final part of the information governance jigsaw is that it is particularly important that the CQC ensures there is sufficient analytic capacity and capability for this important area of work. Having asked the right questions (recommendation 1) and captured the answers (recommendation 2); it will be important to spot trends and identify areas for improvement. An evidence management system enabling CQC to drill down into its inspection evidence would also be of great benefit, but clearly not just in the realm of IG.	**2.3 We will develop knowledge and expertise in a small group of staff (for example, inspectors and specialist advisors) as part of the next phase of inspection. We will also develop and deliver improved training for our inspectors as appropriate.** **2.3 CQC's intelligence work is being further developed so that future inspections can be increasingly intelligence-led. That development will include how best to capture and use trends in the use and governance of information.**

3. We recommend that the CQC enhances its pre-inspection procedures to pay more attention to information governance including the views of people who use services, the public and the IG toolkit.	- **We will make use of intelligence from HSCIC, including the IG Toolkit, and others active in this area.** - **We will expect providers to have internally audited their performance and secured external validation of the quality of their arrangements. We will therefore use the findings from those exercises pre-inspection, including concerns raised by members of staff or people who use services.**
4. We recommend that information sharing and other aspects of information governance should be a key focus of the CQC's "place-based" work.	- **The assessment framework for the Quality of Care in a Place project included information governance.**
5. We recommend that the CQC board acts to ensure that its monitoring of Information Governance is at least as effective in adult social care as in other areas of inspection.	- **This will be reviewed in 2016/17 as part of developing CQC's next phase of inspection.**
6. We recommend that the CQC does more proactively to encourage safer and more effective care by promoting good information governance practices.	- **Our key lines of enquiry include questions on good governance and use of information, which will help identify good practice and areas for improvement. These will be included in inspection reports.** - **We will promote examples of good information governance practices where these are identified by CQC and by HSCIC.**
7. We recommend that the CQC ensures that it has processes in place to liaise more effectively with other organisations in this complex landscape.	- **We currently have over 30 memorandums of understanding (MoUs), joint working protocols (JWPs) and information sharing agreements (ISAs) with key partners, which we regularly review.** - **We will take forward recommendations arising from the data security review, which will ensure a closer working relationship with HSCIC.**
8. We recommend that the CQC Board continues to make arrangements to take advice on Information Governance.	- **The Board will continue to receive reports on our information security and governance arrangements in line with CQC's recommendation to providers.** - **Professor Sir Mike Richards is our Caldicott Guardian. Where appropriate, we will continue to seek advice on information governance.**

9. We recommend that the CQC clarifies how it will take corporate responsibility for ensuring that the organisation fulfils its responsibility to monitor and seek to encourage improvement in the Information Governance practice of health and social care providers.	• **We will be making further improvements following the publication of the data security review.**
10. We recommend that the CQC board should commit to reporting annually in both the State of Care report and the CQC Annual report on how it has discharged its statutory responsibility to monitor and seek to improve the Information Governance practice of health and social care providers.	• **This is now embedded as a feature in CQC's State of Care and annual report, and will feature in future reports to highlight the importance of having good information governance systems, which will enable providers to improve the care provided.**

Appendix C: Regulation 17: Good Governance

Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17

17.—

1. Systems or processes must be established and operated effectively to ensure compliance with the requirements in this Part.
2. Without limiting paragraph (1), such systems or processes must enable the registered person, in particular, to—
    a. assess, monitor and improve the quality and safety of the services provided in the carrying on of the regulated activity (including the quality of the experience of service users in receiving those services);
    b. assess, monitor and mitigate the risks relating to the health, safety and welfare of service users and others who may be at risk which arise from the carrying on of the regulated activity;
    c. maintain securely an accurate, complete and contemporaneous record in respect of each service user, including a record of the care and treatment provided to the service user and of decisions taken in relation to the care and treatment provided;
    d. maintain securely such other records as are necessary to be kept in relation to—
        i. persons employed in the carrying on of the regulated activity, and
        ii. the management of the regulated activity;
    e. seek and act on feedback from relevant persons and other persons on the services provided in the carrying on of the regulated activity, for the purposes of continually evaluating and improving such services;
    f. evaluate and improve their practice in respect of the processing of the information referred to in sub-paragraphs (a) to (e).
3. The registered person must send to the Commission, when requested to do so and by no later than 28 days beginning on the day after receipt of the request—
    a. a written report setting out how, and the extent to which, in the opinion of the registered person, the requirements of paragraph (2)(a) and (b) are being complied with, and
    b. any plans that the registered person has for improving the standard of the services provided to service users with a view to ensuring their health and welfare.

Published April 2016

CareQuality
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 would like a summary of this report in another language or format.