BRIEFING PAPER

Assurance with Vision

Your Data: Better Security, Better Choice, Better Care

July 2016 saw the publication of two reports relating to Information and Cyber Security. The National Data Guardian's (Dame Fiona Caldicott) *Review of Data Security, Consent and Opt-Outs* and the Care Quality Commission report *Safe Data, Safe Care*.

On 12th July 2017 the Department of health published its response , accepting the recommendations made within both reports, and announcing some key changes to the way that Information and Cyber-Security will be managed and assessed.

Headline Messages

The Data Security Standards proposed by the National Data Guardian (NDG) have been accepted.

Leadership is key; this was a headline theme from the NDG and CQC in July 2016, reiterated by the Department of Health response. Chief Executive Officers will be required to **provide an annual *statement of resilience*** confirming standards and requirements are being met.

A **named Executive Board Member** should be responsible for data and cyber-security.

Organisations should have moved away from (or be actively managing) any **unsupported operating systems** by April 2018.

Monitoring and enforcement will take place through the IGT and also through the CQC well-led Inspection regime, commencing in **September 2017**.

The CareCERT programme is intended to be supportive, but will be enhanced to include a process of **unannounced spot checks**, to identify vulnerabilities and support organisations in prioritising actions to mitigate them .

Organisations should have **processes in place** to effectively manage data and cyber-security risks in the same way that they would audit and validate financial integrity and patient safety .

NHS Choices will be replaced in September 2017 by NHS.UK.

A national opt-out model to be implemented from March 2018, to engage the public to understand what their data is used for and by whom, and the choices they can make around its use.

360 Assurance has a clear vision for the delivery of audit and assurance solutions. Our approach is one of Partnership and Collaboration. We work in partnership with you to provide a cost effective, quality driven service that helps you deliver your key priorities.

In this paper:

Your Data: Better Security, Better Choice, Better Care

- New Standards
- Leadership
- New Assessments

Your Data: Better Security, Better Choice, Better Care

"*Boards and staff must take the cyber threat seriously, understand the risk to frontline services, and work pro-actively to maximise resilience*"

The 10 Data Security Standards have been adopted, and in one instance strengthened further, to require organisations to report incidents as soon as possible to the CareCERT Service.

The NHS Standard Contract 2017/18 requires organisations to comply with the NDG Data Security Standards.

Critical CareCERT alerts must be followed up within 48 hours.

Organisations should be moving away from, or actively managing, any unsupported systems by April 2018.

The CQC report (Safe Data, Safe Care) recommendations were also accepted, strengthening the focus on leadership, supporting people and technology.

Chief Executive Officers will be required to provide an annual statement of resilience, confirming that standards and requirements are being met, including a named executive Board member responsible for data and cyber security.

Leadership was a key theme in the 2016 report, reiterated in the government response. Leaders, particularly at Board level, will be key to ensuring that standards are embedded at a local level. Data security simply will not improve without strong Board level leadership, which views and prioritises data security as importantly as financial integrity and clinical safety.

Ensuring that Board are implementing the 10 data security standards will be a factor considered by the CQC and NHS Improvement in decisions to apply their regulatory powers.

The CQC Inspection (well-led) regime will include a focus on information and cyber-security from September 2017.

The IGT is being substantially revised and will be replaced by a redesigned assessment framework. This will assess the extent to which standards are embedded, providing a scorecard of cyber-capability.

Points for Consideration

- What questions should you be asking?
- How 360 Assurance can help you?

What questions should you be asking?

Are we compliant?

- The CQC report set out 'what good looks like' against a range of themes. Have you reviewed/ assessed your arrangements against this good practice?
- The Data Security Standards have been published now for a year. Have you reviewed/ assessed your current arrangements against the Standards and identified where further work is required to achieve compliance?
- Do you have an action plan to address any gaps? Is this monitored within your governance structures, and have identified risks been added to your risk register?

How well do we lead?

- Do you have a named executive Board member responsible for data and cyber security?
- Does your Board demonstrate clearly the leadership and communication required to enable the organisation to implement the Standards?
- Is your Board prepared to be held to account for implementation? Does the board prioritise data security as importantly as financial integrity and clinical safety? Can you demonstrate this through our Assurance Frameworks and Board papers?

How can 360 Assurance help?

360 Assurance has, during the past year, worked with a range of organisations to assess compliance against the Data Security Standards.

We can provide supportive, advisory reviews, to help you understand where further work is required, so that your organisation is well-placed to demonstrate compliance and respond to any future inspection/ assessment.

We can create, host, analyse and feed back surveys of staff that test awareness relevant to information and cyber–security. Independent and anonymous surveys provide a useful mechanism for staff to highlight where they circumvent processes, ensuring that you are informed and can strengthen processes so that staff no longer need to find work-arounds.

We can deliver Board awareness sessions, to support your leadership in understanding the risks and issues around information/ cyber-security.

Response to the National Data Guardian

Summary of the NDG Recommendations & Government Response (in italics)

Data Security

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

2) A redesigned IG Toolkit should embed the new standards, identify exemplar organisations to enable peer support and cascade lessons learned. Leaders should use the IG Toolkit to engage staff and build professional capability, with support from national workforce organisations and professional bodies.
***Agreed**: NHS Digital will implement a redesigned Information Governance Toolkit to support the new standards, testing in 2017 and going live in April 2018.*

3) Trusts and CCGs should use an appropriate tool to identify vulnerabilities such as dormant accounts, default passwords and multiple logins from the same account. These tools could also be also used by the IT companies that provide IT systems to GPs and social care providers.
***Agreed**: The redesigned Information Governance Toolkit will signpost Trusts, CCGs, GP systems suppliers and social care providers, to appropriate tools to identify such vulnerabilities.*

4) All health and social care organisations should provide evidence that they are taking action to improve cyber security, for example through the 'Cyber Essentials' scheme. The 'Cyber Essentials' scheme should be tested in a wider number of GP practices, Trusts and social care settings.
***Agreed**: All health and care organisations will need to provide evidence of their efforts to improve cyber security through the redesigned Information Governance Toolkit, being tested in alpha and beta versions in 2017, prior to being introduced by April 2018. This will be used by organisations themselves and by regulators to assure that data security standards are implemented. We will work with a range of health and care organisations through the redesigned Information Governance Toolkit to assess whether 'Cyber Essentials Plus' meets their needs. We will ensure that the redesigned Toolkit, will signpost organisations towards the appropriate assurance framework for them.*

Response to the National Data Guardian

Summary of the NDG Recommendations & Government Response (in italics)

5) NHS England should change its standard financial contracts to require organisations to take account of the data security standards. Local government should also include this requirement in contracts with the independent and voluntary sectors. Where a provider does not meet the standards over a reasonable period of time, a contract should not be extended.
***Agreed**: We will work with NHS England and through local authorities in England, the LGA and ADASS, to embed the data security standards in contracts where appropriate. The standards are already reflected as requirements in the NHS Standard Contract and GMS Contract for 2017/18 which came into force in April 2017.*

6) Arrangements for internal data security audit and external validation should be reviewed and strengthened to a level similar to those assuring financial integrity and accountability.
***Agreed**: The redesign of the Information Governance Toolkit will provide a platform for strengthened assurance around data security. It is being tested in alpha and beta versions in 2017, prior to being introduced by April 2018.*

7) CQC should amend its inspection framework and inspection approach for providers of registered health and care services to include assurance that appropriate internal and external validation against the new data security standards have been carried out, and make sure that inspectors involved are appropriately trained. HSCIC should use the redesigned IG Toolkit to inform CQC of 'at risk' organisations, and CQC should use this information to prioritise action.
***Agreed**: Data security will form part of CQC's well-led inspection framework from September 2017, which will be supported by information from the redesigned Information Governance Toolkit from April 2018.*

8) HSCIC should work with the primary care community to ensure that the redesigned IG Toolkit provides sufficient support to help them to work towards the standards. HSCIC should use the new toolkit to identify organisations for additional support, and to enable peer support. HSCIC should work with regulators to ensure that there is coherent oversight of data security across the health and care system.
***Agreed**: NHS Digital will work with the primary care community in developing the redesigned Information Governance Toolkit being tested in alpha and beta versions in 2017, prior to being introduced by April 2018. The new service will take into account the relative needs and expectations of organisations of different sizes when considering their data security capability. We expect the redesigned Information Governance Toolkit to facilitate the identification of those organisations in need of additional support.*

Response to the National Data Guardian

Summary of the NDG Recommendations & Government Response (in italics)

9) Where malicious or intentional data security breaches occur, the Department of Health should put harsher sanctions in place and ensure the actions to redress breaches proposed in the 2013 Review are implemented effectively.
***Agreed**: The new 2018 UK data protection legislation will provide a framework for protecting personal data and will impose more severe penalties to deter intentional or reckless misuse of information.*

Consent/ opt-out

10) The case for data sharing still needs to be made to the public, and all health, social care, research and public organisations should share responsibility for making that case
***Agreed**: The Government will work with health, social care, research and public organisations to ensure that the benefits of data sharing are included in future public communications.*

11) There should be a new consent/ opt-out model to allow people to opt out of their personal confidential data being used for purposes beyond their direct care. This would apply unless there is a mandatory legal requirement or an overriding public interest.
***Agreed**: The Government agrees with the need to simplify the means by which people can opt out and will engage fully towards implementing this.*

12) HSCIC should take advantage of changing its name to NHS Digital to emphasise to the public that it is part of the NHS 'family', while continuing to serve the social care and health system as a whole.
***Agreed**: The Health and Social Care Information Centre (HSCIC) was renamed NHS Digital on 1 August 2016 and is already realising the benefits from this change.*

13) The Government should consider introducing stronger sanctions to protect anonymised data. This should include criminal penalties for deliberate and negligent re-identification of individuals.
***Agreed**: We are putting stronger sanctions in place by May 2018, through UK data protection legislation, to protect against anonymised information being re-identified through recklessness or deliberate intent.*

14) The forthcoming Information Governance Alliance's guidance on disseminating health and social care data should explicitly refer to the potential legal, financial, and reputational consequences of organisations failing to have regard to the ICO's Anonymisation Code of Practice by re-identifying individuals.
***Agreed**: The Information Governance Alliance (IGA) will publish anonymisation guidance drawing on the ICO's Code of Practice on Anonymisation in 2018.*

15) People should continue to be able to give their explicit consent, for example to be involved in research.
***Agreed**: We will continue to uphold this principle.*

Response to the National Data Guardian

Summary of the NDG Recommendations & Government Response (in italics)

16) The Department of Health should look at clarifying the legal framework so that health and social care organisations can access the information they need to validate invoices, only using personal confidential data when that is essential.
***Agreed**: The Government will look for an early opportunity to clarify the legal framework by working with the Confidentiality Advisory Group (CAG) to ensure its approvals process under Section 251 of the NHS Act 2006 enables organisations to access the data they need.*

17) The Health Research Authority should provide the public with an easily digestible explanation of the projects that use personal confidential data and have been approved following advice from the Confidentiality Advisory Group.
***Agreed**: The Health Research Authority acknowledges this recommendation and is considering further steps, including a technological solution to make its register more accessible.*

18) The Health and Social Care Information Centre (HSCIC) should develop a tool to help people understand how sharing their data has benefited other people. This tool should show when personal confidential data collected by HSCIC has been used and for what purposes.
***Agreed**: NHS Digital will update its data dissemination register to be more explicit about the purposes that the data they disclose has been used for, and will include the benefit described by the data applicant in their application. By December 2018, people will be able to access a digital service to help them understand who has accessed their summary care record. By March 2020, it will also enable people to use online services to see how their data collected by NHS Digital has been used for purposes other than their direct care.*

Response to the CQC

The CQC Recommendations & Government Response (in italics)

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.
***Agreed**: The communication campaign will target leaders as a key group to support them in taking greater ownership.*

2) All staff should be provided with the right information, tools, training and support to allow them to do their jobs effectively while still being able to meet their responsibilities for handling and sharing data safely.
***Agreed**: Both the communications campaign and the data security training will support staff in meeting their responsibilities.*

3) IT systems and all data security protocols should be designed around the needs of patient care and frontline staff to remove the need for workarounds, which in turn introduce risks into the system.
***Agreed**: This recommendation will be overseen by the National Information Board to ensure new systems reduce security risks while remaining user friendly.*

4) Computer hardware and software that can no longer be supported should be replaced as a matter of urgency.
***Agreed**: Organisations will be expected to update systems and to manage risks where that is not immediately possible. Guidance on removing unsupported software will be issued in July 2017. In autumn 2017, the Chief Information Officer for health and social care will set out further action needed to address technology which risks safe patient care. A framework will be in place to support organisations to move to the latest operating system by March 2018.*

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.
***Agreed**: The new assurance framework will put data security onto a similar footing to financial integrity and accountability.*

6) CQC will amend its assessment framework and inspection approach to include assurance that appropriate internal and external validation against the new data security standards have been carried out, and make sure that inspectors involved are appropriately trained.
***Agreed**: The Government welcomes the inclusion of data security in the CQC's well-led inspection framework.*

Further reading

National Data Guardian Review of Data Security, Consent and Opt-Outs, available from www.gov.uk/government/organisations/national-data-guardian

Care Quality Commission Safe Data: Safe Care, available from www.cqc.org.uk/content/safe-data-safe-care

Your Data: Better Security, Better Choice, Better Care, available from https://www.gov.uk/government/consultations/

Cyber Essentials, available from www.cyberessentials.org

10 Steps to Cyber Security, available from www.cesg.gov.uk/10-steps-cyber-security

Assurance with Vision

Contact Us

Call for more information about our services.

0116 225 6114

Visit us on the web at www.360assurance.co.uk

360 Assurance:
Riverside House
Bridge Park Road
Thurmaston
Leicester
LE4 8BL

360 Assurance:
Stapleford Care Centre
Church Street
Stapleford
Nottingham
NG9 8DB

360 Assurance:
Oak House
Moorhead Way
Bramley
Rotherham
S66 1YY

Key Contacts

Andy Mellor, Assistant Director ☎ 07775 007 154
✉ andy.mellor@nhs.net

Simon Gascoigne, Deputy Director ☎ 0115 883 5305

Leanne Hawkes, Deputy Director ☎ 01709 428 713