360 ASSURANCE

BRIEFING PAPER

Assurance with Vision

Information and Cyber-Security

July 2016 saw the publication of two long-awaited 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*.

This paper attempts to consolidate over 90 pages of findings, key messages and recommendations, into a digestible summary—highlighting in particular *what this means for you*, and how 360 Assurance can help.

Headline Messages

Both reports emphasise the need for strong leadership, not just restricted to the Senior Information Risk Owner (SIRO) and/ or the Caldicott Guardian, but by the whole Board. Every organisation needs to demonstrate the same ownership and responsibility for data security as it does for clinical and financial management and accountability.

The reports focus on outdated technology, which is identified as posing risk to security, and hampering safe, effective and efficient operating processes. This could have significant cost implications for organisations.

Organisations will require greater internal and external scrutiny to demonstrate that Data Security Standards are being met.

The Information Governance Toolkit (IGT) will be revised significantly, to avoid being a tick-box exercise. It will support organisations to meet new Data Security Standards, but also be used by the CQC to identify 'at risk' organisations.

There will be a greater focus on Data Security within CQC Inspections, together with harsher sanctions for those organisations where data security breaches occur.

The question of consent and opt-outs remains complex, and the National Data Guardian concludes that there is a need for communication and further consultation before making any changes to existing arrangements. Two models are provided however, indicating what a 'single question' and 'two-question' opt-out might look like.

360 ASSURANCE

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:

- Key messages from the National Data Guardian and Care Quality Commission
- National Data Guardian Report: Summary
- Care Quality Commission Report: Summary
- How 360 Assurance can help you

August 2016

National Data Guardian for Health and Care: Review of Data Security, Consent and Opt-outs.

The National Data Guardian Report in Numbers

- **Twenty** Recommendations
- **Three** Leadership Obligations
- **Ten** new Data Security Standards

"*This is a report about trust*"

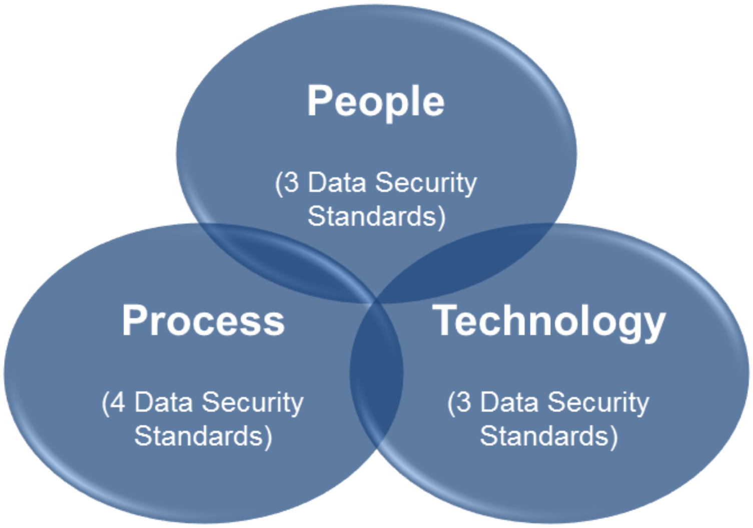
The report's opening words set the scene for the review and Dame Fiona outlines what she was asked to do by the Secretary of State for Health:

- to recommend new Data Security Standards;
- to recommend a method for testing compliance with these standards;
- to recommend a new consent or opt-out model.

In response the review questions whether current security is good enough, and do people understand when their data is shared? It investigated a simple opt-out to restore public trust, to ensure that patients were not surprised when data was shared, and to ensure that only the minimum amount of data necessary is shared.

The report notes that there are already many standards in place, but that they have disadvantages. The IGT is treated by many as a tick-box exercise; the Cyber Essentials scheme has not been widely used within the Health Sector, and ISO accreditation is complex and expensive.

The new Data Security Standards are designed to be simple to understand and follow, but they require leadership across the Board. The ten new standards are set out within *Leadership Obligations*, framed around people, process and technology:


People
(3 Data Security Standards)
Process
(4 Data Security Standards)
Technology
(3 Data Security Standards)

Points for Consideration

- Are people equipped to handle information?
- Do leaders demonstrate clear ownership and responsibility for data security?
- Are staff trained and supported effectively?

Data Security

The NHS has a high degree of public trust, but this is being eroded by data breaches. Public confidence would be restored through harsher sanctions coupled with regular assessment of compliance through the existing inspection regime.

The review notes that data security is often seen as the responsibility of the SIRO and/ or the Caldicott Guardian rather than as a collective Board responsibility.

Historically breaches have related to hard copy medical records and faxes. Many have been unwittingly facilitated by the behaviours of employees motivated to get their job done and hampered by inefficient or outdated technology.

As systems and records are digitised the cyber-threat increases, with the potential for large-scale loss or leakage of data, in contrast to past breaches which have tended to be limited to a smaller number of hard copy records.

There is plenty of guidance available, but if anything data controllers are confused by the plethora of standards and unsure which to follow. The new Data Standards will provide a simple and definitive set of guidance for data security across health and social care.

People: ensure staff are equipped to handle information

Those who work in health and social care want to provide the best possible care, but their behaviour is often the unintentional cause of breaches. Often this arises from naivety—sometimes from negligence but with a failure to detect poor behaviours or to hold individuals to account.

***Data Security Standard 1**: All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes*

In terms of data sharing, a lack of understanding and awareness often causes people to default to risk avoidance and an unwillingness to share. There is a concern that the recipients of data cannot be trusted, due to poor or unknown security standards. The IGT will be redesigned to embed the new Standards, and also to identify exemplar organisations. Leaders should use the toolkit to engage staff and build professional capability.

***Data Security Standard 2**: All staff understand their responsibilities under the National Data Guardians Data Security Standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.*

Points for Consideration

- Do you train and support all staff appropriately?
- Do you have a learning culture, rather than a blaming culture?
- Do your processes support or hamper staff?

The review identified a culture of blaming rather than learning, which prevented staff from speaking up when they were aware of near misses, hazards and insecure behaviours.

The review identified simple errors caused by heavy workloads, together with negligent behaviours where staff were not held to account. The review highlights that consistent training, education and awareness were vital to addressing behavioural issues.

***Data Security Standard 3**: All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.*

Process: ensure that the organisation proactively prevents data security breaches and responds to incidents

When processes are poorly designed people revert to doing something in the most convenient way.   Security needs to be seen as an enabler rather than a blocker. Fundamental tasks such as the management of starters and leavers were hindered through ineffective communication, resulting to workarounds for new starters, and dormant accounts relating to leavers.

***Data Security Standard 4**: Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.*

The review highlighted a view that systems do not support frontline staff - "*IT security need to walk in the shoes of a clinician for a day*".   The review highlighted tensions between attempts to follow the security processes balanced against the practicalities of needing to access information.

***Data Security Standard 5**: Processes are reviewed at least annually to identify & improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.*

The review notes the need to use technology effectively to support data security. It provides an example of a vulnerability analysis tool (The Palantir Dashboard) which answers simple questions around users, suggesting that 80% of vulnerabilities can be addressed with 20% of effort. Ensuring a safe ongoing 'cyber-posture' and responding promptly to incidents is key.

***Data Security Standard 6**: Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.*

Points for Consideration

- Are you prepared?
- Do you have plans in place and clarity on how to respond to a data incident - have they been tested?
- Is your technology up to date?
- How do you ensure your systems are protected?
- Do you hold your suppliers to account?

Organisations should plan ahead and know what they intend to do in the event of a threat do data security, including data breaches and near misses. Continuity plans should be developed and tested.

***Data Security Standard 7**: A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses; it is tested once a year as a minimum, with a report to senior management.*

Technology: ensure technology is secure and up to date

Technology can be an enabler, but also a source of risk when it is out of date and unsupported. Local IT systems are ageing and unsupported. This means that they cannot be patched to maintain as secure. Some systems were not designed to feature modern security controls, or to handle large volumes of data. When security controls are applied to older technologies, the resulting procedures can be counter-intuitive, inconvenient and easy to get wrong.

***Data Security Standard 8**: No unsupported operating systems, software or internet browsers are used within the IT estate.*

Organisations should be aware of their cyber-posture, and areas of vulnerabilities. The CESG (GCHQ's Information Security arm) *10 Steps to Cyber Security* highlights main areas of vulnerability, with the *Cyber Essentials* Scheme launched to standardise the implementation of an affordable protected IT Infrastructure. The use of Cyber Essentials has been limited to date within the health and social care sectors.

***Data Security Standard 9**: A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.*

Organisations clearly have a responsibility for ensuring that the technology in use it maintained up to date, is monitored and tested routinely. In many instances data may be processed by external suppliers, or organisations may be reliant on suppliers identifying vulnerabilities and providing security patches.

***Data Security Standard 10**: IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standard.*

Points for Consideration

- Compliance will be monitored through Inspection
- The IGT will be used to identify organisations at risk
- How will you obtain internal and external assurance and validation?

Embedding the Standards

The review notes that, to embed standards, they must be **enforced within contracts**. Therefore the NHSE is recommended to change financial contracts to require organisations to take account of the data security standards.

Organisations should provide objective, third party **assurance of compliance** with standards for example through Internal Audit. Arrangements for internal review and external validation should be strengthened to a level similar to financial integrity and accountability.

Review of data security arrangements will be **integrated into inspection**. The CQC is to integrate measures into Well-Lead, amending the inspection framework and approach to include assurance that internal and external validation against new data standards is being carried out.

Organisations should be **learning and not blaming**, with the IGT used to identify organisations in need of support, and those exemplary organisations that can provide it.

Where there are breaches, there will be **harsher sanctions**. The Department of Health will ensure that actions are in place to redress breaches flagged in existing reports, with more severe consequences where an organisation consistently fails to remedy situations going forward.

Consent/ Opt-out of information sharing

The review notes that opt-outs already exist, for example Type 1 (information held by a GP not to be shared outside the GP Practice) and Type 2 (confidential information not to leave the HSCIC in an identifiable form). The review notes that these are not understood, and there is a need for a simpler opt-out. But it also concludes that further consultation is needed, and whilst it provides illustrative opt-outs, using a single-question and two-part approach, it does not indicate a preferred way forward.

The report does indicate that, irrespective of the nature of any future question, de-identified (aka pseudonymised) information need not be subject to opt-out. The review noted that there is already sufficient guidance and penalties in place, and public support for the use of anonymised and pseudonymised data as an impetus to moving away from personally identifiable data.

The review returned to the importance of trust - most people do not feel the need to know what is happening with their data, and they want to be able to ’trust the system’.

Points for Consideration

- Further public communication and consultation is required
- The case for data sharing still needs to be made
- All organisations share a responsibility for making that case

People should be made aware of the use of their data and the benefits, with an opt-out model for those with concerns.

The case for data sharing still needs to be made and organisations need to share the responsibility for making that case.

There should be no surprises for an individual about who has access to information about them.

Data is currently used for a number of purposes beyond the provision of direct care. Examples include commissioning, monitoring the provision of services, assessing wider public health, and research. The review identified support for the use of such data for running health and social care, when the benefits of doing so are explained. There remains a distinction of views relating to the NHS family and others making use of such data.

A two-question opt-out would allow people to distinguish between the sharing of information for the provision of local services and running the health and social care system, with a second covering research to improve treatment and care. A single question might be deemed simpler, but could limit people's choice.

There are currently inconsistencies in the amount and nature of information shared within the NHS family - the review suggested that data be passed to (what was then) HSCIC as the statutory safe haven to de-identify or anonymise data for sharing with those that need to use it. The review highlights the opportunity arising from the HSCIC's name change to NHS Digital, to reinforce to the public that it is part of the NHS family.

Best practice is already available from the Information Commissioner's Office (ICO), which should be used to safeguard data, together with tougher sanctions for breaches. Guidance is anticipated from the Information Governance Alliance on disseminating health and social care data, and this should refer explicitly to the consequences of organisations failing to have regard to the ICO Code of Practice, and re-identifying individuals.

The review acknowledged the need to share information for invoicing purposes, for example if a patient taken ill and treated out of their CCG area. The public are generally not concerned with this, as the data is not shared outside the NHS family, but the Department of Health should clarify the legal framework so that organisations can access information to validate invoices.

The review proposed further consultation with the public, recognising the size of the task and the fact that extensive and ongoing communication is required. Patients should be assured that their information will never be used for marketing or insurance purposes.

The Health Research Authority is recommended to provide a digest of projects that use personal data, whilst the HSCIC should develop a tool to help people understand how sharing data has benefited others.

The public are likely to be provided with a set of eight statements to help them understand how their data is protected.

Points for Consideration

- The National Data Guardian's 20 recommendations

Summary of the National Data Guardian's Recommendations

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.

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.

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.

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.

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.

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.

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.

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.

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.

Points for Consideration

- The National Data Guardian's 20 recommendations

Summary of the National Data Guardian's Recommendations

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

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.

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.

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.

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.

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

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.

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.

18) The Health and Social Care Information Centre (HSCIC) should develop a tool to help people understand how sharing their data has benefited other people. This tool should show when personal confidential data collected by HSCIC has been used and for what purposes.

Next Steps

19) The Department of Health should conduct a full and comprehensive formal public consultation on the proposed standards and opt-out model. Alongside this consultation, the opt-out questions should be fully tested with the public and professionals.

20) There should be ongoing work under the National Information Board looking at the outcomes proposed by this consultation, and how to build greater public trust in data sharing for health and social care.

The CQC Report
Safe Data: Safe Care

Points for Consideration

- The profile of data security needs to be raised
- Leaders should be accountable, staff should be trained and supported
- Organisations should learn from each other
- Systems should be designed around the needs of frontline staff

Good information underpins good care.

Patient safety is only assured when information is accessible, integrity is protected and confidentiality is maintained. Data security needs to be treated very seriously and has been pushed to the forefront of public attention following recent high profile data breaches.

The CQC was asked by the Secretary of State for Health to:

- review the effectiveness of current approaches to data security by NHS organisations and recommend how providers can improve; and
- recommend how the guidelines published by the NDG can be assured through inspection, commissioning and other potential mechanisms.

Poor practice exists that could have led to data breaches; complacency must be avoided and new technology introduces new risks.

Organisations must **understand their exposure** to risk; leadership of organisations must **prioritise information security**, including **testing policies** in the same way that an organisation would test alarms and evacuation procedures. NHS **leaders should be accountable** in the same way that they would for clinical and financial management and accountability.

Data security is defined within the review using the (long-accepted model) of Confidentiality, Integrity and Accessibility. As with the National Data Guardian’s report, the review found widespread commitment to data security, but challenges in translating commitment into reliable practice.

Data incidents taken seriously but staff don’t feel that lessons are learned or shared effectively;

Staff training is variable at all levels, including up to SIRO and Caldicott Guardians.

Policies and procedures are generally in place – but day to day practice does not reflect adherence.

Benchmarking with other organisations virtually absent – there is no culture of learning from others, or checking/ validating arrangements with others.

Technology is growing for recording and storing patient information, but unless accompanied by improvement this creates a risk of more serious large scale data losses.

Data security systems not designed around the needs of frontline staff, leading to insecure workarounds.

Development of integrated patient care needs to be accompanied by improvements in the ease of sharing data between services

Points for Consideration

- Summary of recommendations
- The CQC lines of enquiry are consistent with the National Data Guardian themes of People, Process and Technology

The CQC Recommendations

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

Three Key Lines of Enquiry

The CQC's review was structured around three lines of enquiry:

- How well does the leadership enable staff to keep information secure?
- How well do processes ensure the right levels of security?
- How well does an organisation equip itself to keep secure (paper, hardware and software)?

The CQC noted from existing data that the majority of breaches to date have involved paper records rather than digital breaches, and indicates that patient data is not currently the highest priority for targeted attack by cyber criminals. But also notes that this does not mean that the risk won't increase in future.

The report observed from HSCIC's 2014 Strategic Data Assurance Report that areas for improvement included the need to ensure secure configuration of hardware and software, something that will not be possible if organisations use systems that are no longer supported (for example Windows XP).

Points for Consideration

- What good looks like

What does good look like?

Helpfully, the CQC report sets out 'what good looks like' - this should help organisations to have something to work towards, and something against which existing gap analysis can be framed.

Leadership

There should be visible and active leadership, demonstrating clear ownership in the same way as for financial management and accountability.

Organisations test and understand the exposure to risk, seeking out independent, external validation of their data security.

Leaders recognise that outsourcing services does not outsource their responsibility.

Leaders and organisations create a culture where it is easier to maintain data security than not.

The report warns that "*many leaders see data security as the job of the IT department*" - this is not the case!

Training

Training is mandatory and refreshed regularly for all staff (including temporary and agency). It is also tailored to recipients so that it has the greatest impact.

Staff should be trained how to access and share information remotely, and they should understand how to work safely in environments that don't lend themselves to privacy.

It is not possible to cover everything within training (or to expect staff to remember everything that they are told). Organisations should ensure that staff are clear about where to find reliable guidance quickly and easily.

It is essential that senior staff (including but not restricted to the SIRO and Caldicott Guardian) are properly trained and kept up to date.

Patient access to their own data

Patients should be well informed and understand *what* they can and cannot share.

Patients should be advised *how* to protect their own data online or in discussion.

Staff access to patient records

Access is set according to what staff *need* to do their job (least privilege).

Access is controlled and withdrawn promptly when staff change roles or leave an organisation.

Attempts to access secure systems are treated with caution.

Logins are controlled and unique, with appropriate password controls.

Smart cards are unique where they are used, they are issued and cancelled promptly when someone leaves.

Points for Consideration

- What good looks like

What does good look like?

Mobile and Remote Working

Staff are provided with encrypted devices (where appropriate) to enable them to work safely and effectively onsite or offsite.

Staff are trained how to work securely, so they are able to keep data safe without compromising their ability to access data when needed.

Learning and Benchmarking

Organisations take the opportunity to learn and share from others with similar challenges.

Organisations compare performance with others as a way to maintain improvement and stimulate innovation.

Business Continuity

Organisations should recognise and plan for emergencies (in the context of cyber-incidents and data breaches), developing and practicing plans for continuity and return to normality.

Control of removable records

Well lead organisations avoid anything being unlocked or unattended, from paper to USB/ removable drives. Records are not left or processed (where avoidable) in public areas and they are locked away security.

Access to data and data sharing

Staff have access to data when and where necessary to support patient treatment.

Data is shared quickly, effectively and safely with those involved in care, including across organisations.

Staff understand the importance of sharing data and are assured they can do so safely.

Organisations are supported to work together to agree common arrangements for data sharing.

IT Security

IT systems are supported and maintained, and tested regularly to confirm that they are fit for purpose. Results of testing are shared regularly with the organisation's leadership.

Security is designed around the needs of patient care and front line staff.

Organisations develop plans that maintain security and access while supporting closer integration.

Points for Consideration

- Gap assessments against CQC's *good practice* models
- Assurance audits to provide the internal challenge and validation required
- Staff surveys, to assess awareness and test for work-arounds
- Validation of Data Security Standards
- Review of dormant accounts and system security
- Support for Cyber Essentials

How can 360 Assurance help?

The two reports provide extensive research, commentary and recommendations for organisations that will drive improvement in data and cyber-security arrangements. However there is clearly much work for you to do. The blitz on outdated technology could be costly, and significant resources will be required to implement the new Data Security Standards and to act on the recommendations of the reports.

These reports make reference to increased external scrutiny. We have assessed the areas where you my need immediate help and ways in which 360 Assurance can support you in responding to the actions arising from the reports.

Gap assessments: The CQC has helpfully set out 'what good looks like'. You should be aspiring to meet the behaviours identified and we can assess your existing arrangements against the suggested good practice, highlighting the actions needed to strengthen existing arrangements.

Assurance audits: You will be required to obtain internal and external challenge and validation, and the CQC Inspection Regime will look for evidence of this going forward. As part of planning for future years, or during periodic reviews of existing plans, we can incorporate audit reviews that will provide the challenge and assurance that you need, where appropriate themed across People, Process and Technology.

Staff surveys: You will be required to provide training and support to staff, and to ensure that this is relevant to their needs it is important that you understand existing awareness. We can create, host, analyse and feed back surveys of staff that test awareness of internal policies and procedures - and wider issues - relevant to information and cyber–security. Independent and anonymous surveys often provide a useful mechanism for staff to highlight where they circumvent processes, ensuring that organisations are informed and can strengthen processes so that staff no longer need to find work-arounds.

Validation of Data Security Standards: You will be required to meet the new Data Security Standards and we can assess your progress towards meeting the standards and assess your levels of compliance. Our approach will provide constructive challenge and assurance regarding the progress made and the actions that might be needed for ensure full compliance.

Review of accounts and system security: You will be required to analyse your systems and records to identify dormant accounts and to assess the strength of security across your systems. We can undertake analysis on your behalf or review your arrangements, helping you to respond directly to one of the key recommendations within the National Data Guardian's report.

Cyber Essentials: You will be required to assess your arrangements against the Cyber Essentials framework, and where appropriate seek accreditation with this scheme. We can provide challenge and support to help you to meet these requirements.

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

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

Annette Tudor, Deputy Director	0116 225 6124
Simon Gascoigne, Deputy Director	0115 883 5305
Leanne Hawkes, Deputy Director	01709 428 713
Andy Mellor, IMT Lead	01709 428 725