NHS Digital

Data Security Standards

Overall guide

The bigger picture of where the standards fit in

2018

Information and technology
for better health and care

Contents

Overview

The National Data Guardian's (NDG) Data Security Standards are intended to apply to every organisation handling health and social care information, although the way that they apply will vary according to the type and size of organisation. For example, GPs may want support from their system suppliers to identify and respond to cyber alerts in the first instance, and many social care organisations will want that from their Local Authority. Commissioners should take account of the standards when commissioning services.

"Leaders of all health and social care organisations should commit to the following data security standards. They should demonstrate this through audit or objective assurance and ensure that audit enables inspection by the relevant regulator."

The Standards

What are they?

The National Data Guardian's Review of Data Security, Consent and Opt-Outs has set out ten data security standards clustered under three leadership obligations to address people, process and technology issues:

Leadership Obligation 1: People: ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

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

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

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

Leadership Obligation 2: Process: ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

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

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

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

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

Leadership Obligation 3: Technology: ensure technology is secure and up-to-date.

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

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

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

The assertions and evidence

The assertions sit under each standard and represent a specific theme related to that standard. Evidence items sit under assertions and represent specific pieces of evidence that would be an indicator of maturity in that area.

For example:

Data Standard 9 IT protection	• 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
Assertion 9.4	• A data security improvement plan has been put in place on the basis of the assessment and has been approved by the SIRO.
Two of the evidence items	• What are your top three data security and protection risks? • Evidence that your board, or equivalent, has discussed your top three data security and protection risks and what is being done about them, in the last twelve months?

In this example, standard 9 has multiple assertions, of which 9.4 is concerned with senior ownership and the two evidence items are concerned with identifying your top three data security and protection risks and presenting them to a high-level body.

The standards and assertions are not as prescriptive as the predecessor standard contained within the information governance toolkit. In this example, to present the top three risks you would have to have the following in place:

- a method of capturing your risks
- a method of analysing your risks
- a method of ranking your risks
- a method of management and treatment of those identified risks
- your high-level body is engaged with data security and protection
- a plan to check act methodology for continuous improvement on risk issues.

Unlike the previous information governance standard, the new standards, assertions and evidence are not intended to be a complete framework for data security and protection.

> The standards, assertions and evidence items are not intended to be a complete framework to manage data security and protection. They represent indicators of good practise and maturity.
>
> NHS Digital

Ideally, the evidence items should fall out from your existing management arrangements. If you find yourself creating evidence just to comply with the standard, you are probably doing the wrong thing.

Sometimes under the old regime, organisations created policies, processes, procedures and minutes that existed just as evidence, not connected to reality and not used to drive forward improvement.

So, it is important that the frameworks you use encompass the new standards and are not separate.

This guide sets out some of the frameworks that can help you.

The Data Security and Protection Toolkit

The Data Security and Protection (DSP) Toolkit is an online self-assessment tool that enables organisations to measure and publish their performance against the National Data Guardian's ten data security standards. It has been updated and improved to be more user-friendly and accessible.

The DSP Toolkit will retain the general principle that organisations should demonstrate that they can be trusted with the confidentiality and security of personal information. It will also support the key requirements under the General Data Protection Regulation (GDPR), as identified in the NHS GDPR Checklist.

The standards, assertions and evidence items are all contained within the DSP Toolkit, range of assertions changes dependant on your organisation type and circumstances of your processing.

Frameworks

There are many industry frameworks that may help with your data security and protection responsibilities.

Some are general and some target specific areas. Even the most extensive (such as ISO 27001) will not cover all your security and protection responsibility.

> Not any one industry framework will cover all your data security and protection responsibilities
>
> NHS Digital

The frameworks examined are:

- ISO 27001
- ISO 9001
- Cyber Essentials / Cyber Essentials +
- Public Services Network (PSN) Compliance
- other frameworks.

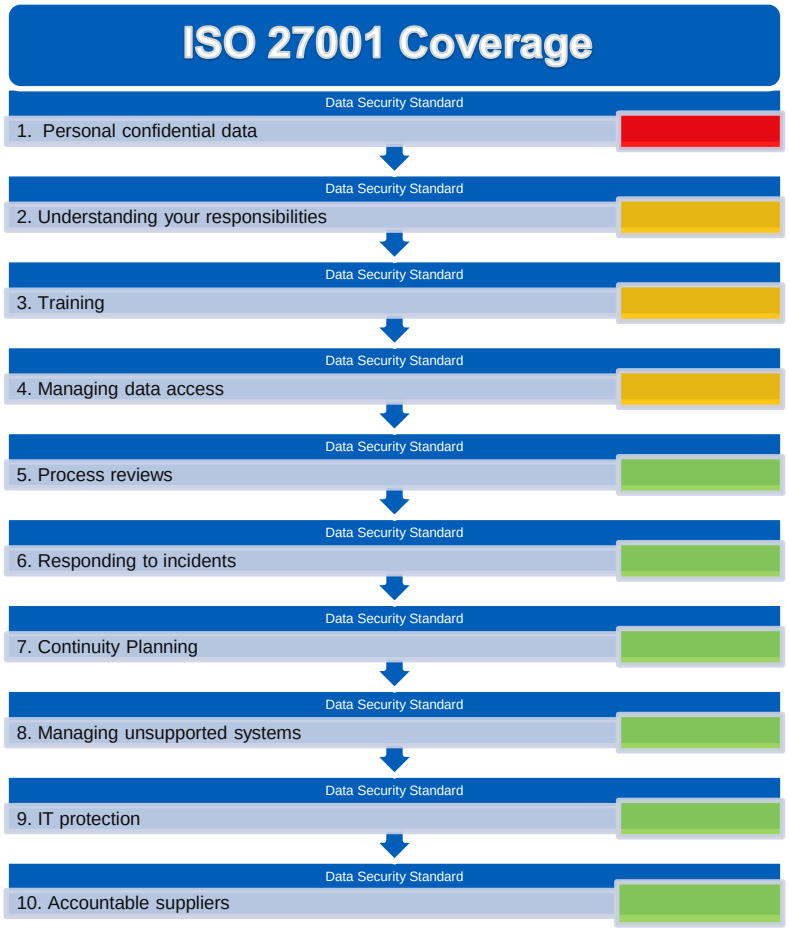
ISO 27001

The ISO/IEC: 27000 series of standards are recognised internationally as an effective and comprehensive standard. Most organisations using this standard seek accreditation of their implementation as a means of demonstrating to customers, stakeholders, regulators and others that information security has been independently assessed and validated.

However, having an in-date scoped certification that covers your health and care processing means you will have equiveillance with certain assertion and evidence. The diagram below offers a high-level view of equiveillance coverage and with the DSP Toolkit you are required to complete fewer items.

> Warning: If your certification covers your IT department and you process health and care social beyond that, you will not have coverage
>
> NHS Digital

See the detailed coverage guide here



Red little = little / no coverage Amber = Some coverage Green = Significant Coverage

ISO 9001

The ISO/IEC: 9000 series addresses various aspects of quality management and contains some of ISO's best-known standards. The standards provide guidance and tools for companies and organisations which want to ensure that their products and services consistently meet customers' requirements, and that quality is consistently improved.

This standard is not data security or protection centred 'out-of-the-box', as it is designed to produce a quality management system. However, your quality management system could encompass a security management framework.

As this standard implementation is bespoke and dependent on your defined quality management system, mapping to the data security standards is not possible. However, a quality management system in tandem with security standards should produce a wealth of evidence due to the documentary nature of the standard.

ISO 9001 can also be useful in plugging the gaps from other standards to encompass the whole of the data security standards as a wrapper.

Cyber Essentials / Cyber Essentials +

Under this scheme, which is backed by Government and supported by industry, organisations can apply for certification, which recognises the achievement of government-endorsed standards of cyber hygiene. There are two levels of certification:

- Cyber Essentials Badge

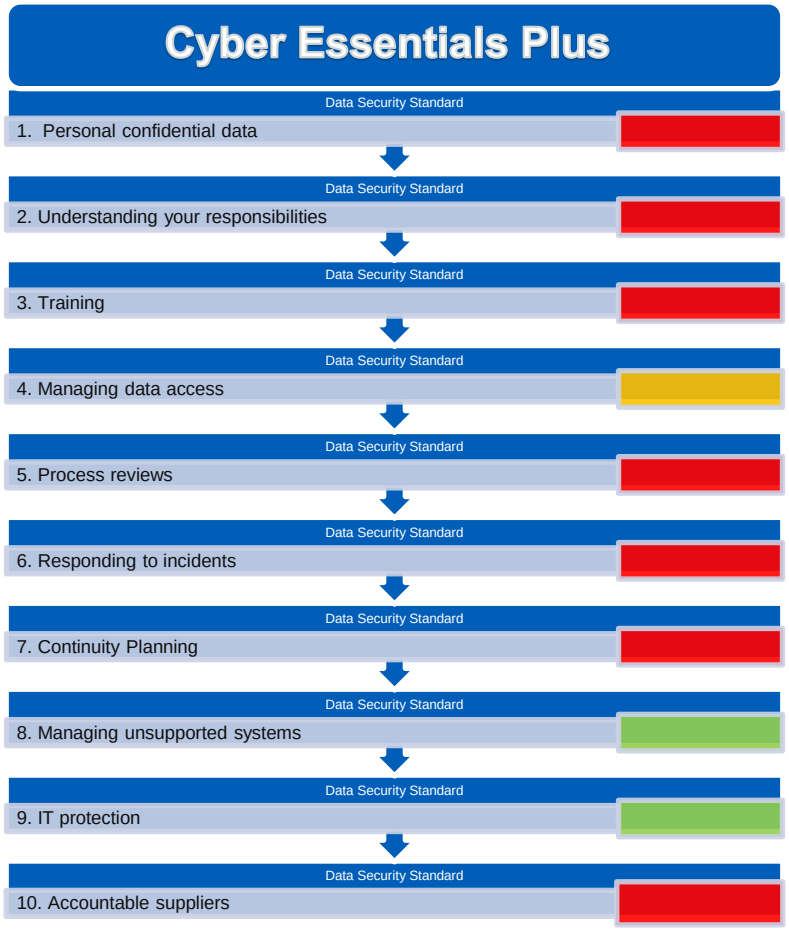
Cyber Essentials – organisations complete a self-assessment questionnaire and the responses are reviewed by an external certifying body.

- Cyber Essentials Plus Badge

Cyber Essentials Plus – tests of the organisation's systems are carried out by an external certifying body.

> Cyber Essentials plus will give you equivalence under the DSP Toolkit
>
> NHS Digital

See the detailed coverage guide here



Red little = little / no coverage Amber = Some coverage Green = Significant Coverage

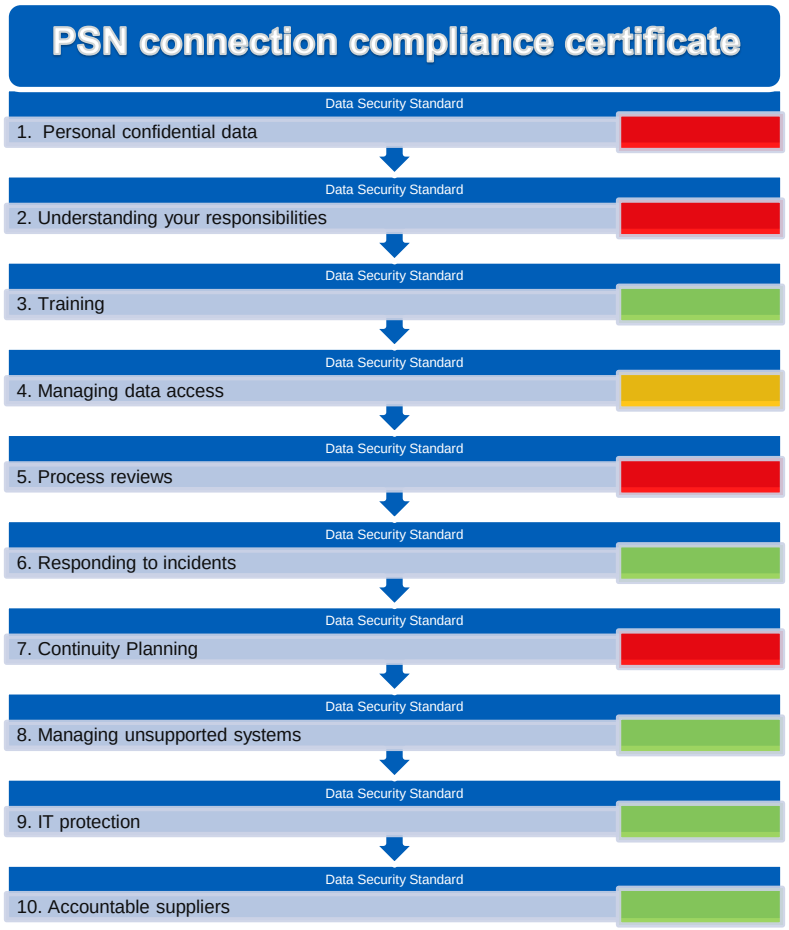
Public Services Network (PSN) Compliance

The PSN is the government's high-performance network, which helps public sector organisations work together, reduce duplication and share resources. PSN compliance is a way to report your security arrangements. It is how you demonstrate to central government that your organisation's security arrangements, policies and controls are sufficiently rigorous for us to allow you to interact with the PSN and those connected to it.

Generally, most of the organisation subject to PSN compliance interacting with the health and care system will be local authorities. The method to demonstrate assurance is through a Public Services Network (PSN) connection compliance certificate.

> A valid in date PSN connection compliance certificate is required to claim equivalence with the DSP Toolkit
>
> NHS Digital

See the detailed coverage guide here



Red little = little / no coverage Amber = Some coverage Green = Significant Coverage

Other frameworks

There are a range of other frameworks that can be used support to support a data security and protection assurance. These range from security centric ones, such as NIST SP 800 Series or Cybersecurity framework to the more general ISACA's Cobit Methodology. There is compliance framework around the payment card industry (PCI) and companies dealing with the US government with Sarbanes Oxley compliance.

US based healthcare suppliers my claim HIPPA and Hitech compliance. All this framework and legislation compliance (mostly US) produces incredibly useful evidence but there is no direct equivalent to the data security standards.

Appendix 1 - Left Blank

Appendix 2 - Useful resources

ISO/IEC 27000 family - Information security management systems: International Organisation for Standardisation

A description and link to the ISO 27000 family of standards

https://www.iso.org/isoiec-27001-information-security.html

ISO 9000 - Quality management: International Organisation for Standardisation

The ISO 9000 family addresses various aspects of quality management and contains some of ISO's best-known standards. The standards provide guidance and tools for companies and organizations who want to ensure that their products and services consistently meet customer's requirements, and that quality is consistently improved.

https://www.iso.org/iso-9001-quality-management.html

Cyber Essentials : National Cyber Security Centre

Cyber Essentials helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security

https://www.cyberessentials.ncsc.gov.uk/

Public Services Network (PSN): Government Digital Service

The PSN is the government's high-performance network, which helps public sector organisations work together, reduce duplication and share resources.

https://www.gov.uk/government/groups/public-services-network

Cybersecurity Framework: National Institute of Standards and Technology U.S. Dept of Commerce

A US federal framework directed from an executive order "Improving Critical Infrastructure Cybersecurity."

https://www.nist.gov/framework

NIST 800 Series: National Institute of Standards and Technology U.S. Dept of Commerce

The NIST 800 Series is a set of documents that describe United States federal government computer security policies, procedures and guidelines.

https://www.nist.gov/

COBIT: ISACA

The COBIT 5 framework for the governance and management of enterprise IT is a leading-edge business optimisation and growth roadmap that leverages proven practices, global thought leadership and ground-breaking tools to inspire IT innovation and fuel business success.

http://www.isaca.org/cobit/pages/default.aspx

Payment Card Industry (PCI): The PCI Security Standards Council

The PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

https://www.pcisecuritystandards.org/

Sarbanes Oxley The Laws That Govern the Securities Industry: U.S. Securities and Exchange Commission

Guide to the Sarbanes-Oxley Act of 2002 (US).

https://www.sec.gov/answers/about-lawsshtml.html#sox2002

HIPPA (US) Health Information Privacy: U.S. Department of Health and Human Resources

Guide to HIPPA rules and compliance.

https://www.hhs.gov/hipaa/index.html

HITECH Act: U.S. Department of Health and Human Resources

US healthcare act to promote the adoption and meaningful use of health information technology.

https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html

Appendix 3 –
Data security reports

The National Data Guardian review

Recommendations to improve security of health and care information and ensure people can make informed choices about how their data is used.

Review of Data Security, Consent and Opt-Outs

The government response

'Your Data: Better Security, Better Choice, Better Care' is the government's response to:

- the National Data Guardian for Health and Care's 'Review of Data Security, Consent and Opt-Outs';
- the public consultation on that review;
- the Care Quality Commission's Review 'Safe Data, Safe Care'.

It sets out that the government accepts the recommendations in both the National Data Guardian review and the Care Quality Commission review.

It also reflects on what we heard through consultation to set out immediate and longer-term action for implementation.

Your Data: Better Security, Better Choice, Better Care