NHS Digital

Data Security Standard 2

Staff responsibilities

The bigger picture and how the standard fits in

2019/20

Information and technology for better health and care

Contents

Overview 3

Systems holding personal confidential & sensitive information 4

Definitions and scope 4
SIRO, IAO, IAA, IA structure 5
List of systems holding Personal Information 6
SIRO involvement 6
Data protection and security induction 7
Delivery of the induction 8
Staff scope 8
Review 8
Staff contracts 9
An improving picture 9
Appendix 1 - 10
Table of Data Security Level 2 Assertions 10
Appendix 2 - 11
Useful resources 11
Appendix 3 – 12
The National Data Guardian Reports 12

Overview

The National Data Guardian (NDG) review's data standard 2 states that:

"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."

All staff understand what constitutes deliberate, negligent or complacent behaviour and the implications for their employment. They are made aware that their usage of IT systems is logged and attributable to them personally. Insecure behaviours are reported without fear of recrimination and procedures which prompt insecure workarounds are reported, with action taken.

Systems holding personal confidential & sensitive information

Definitions and scope

Personal confidential information (PCI) is personal and sensitive confidential information that is held by your organisation and is subject to an obligation of confidentiality, relating to staff and patients / service users. Confidential personal information is likely to include (but is not limited to) information about a person's:

- physical or mental health
- social or family circumstance
- financial standing and financial details
- education, training and employment experience
- religious beliefs
- racial or ethnic origin
- sexuality
- criminal convictions
- genomic data
- IP address.

Confidential personal information would be held in systems such as:

- patient administration systems
- staff rostering systems
- payroll
- theatre systems
- data warehouses
- a clinical correspondence system.

For the purposes of the NDG standards, a system is defined as usually being digital and would hold 10% or more of employed staff or 10% or more of the volume of patients PCI.

Organisational sensitive information is also included such as service redevelopment and reorganisation, financial and cyber security information that could be exploited

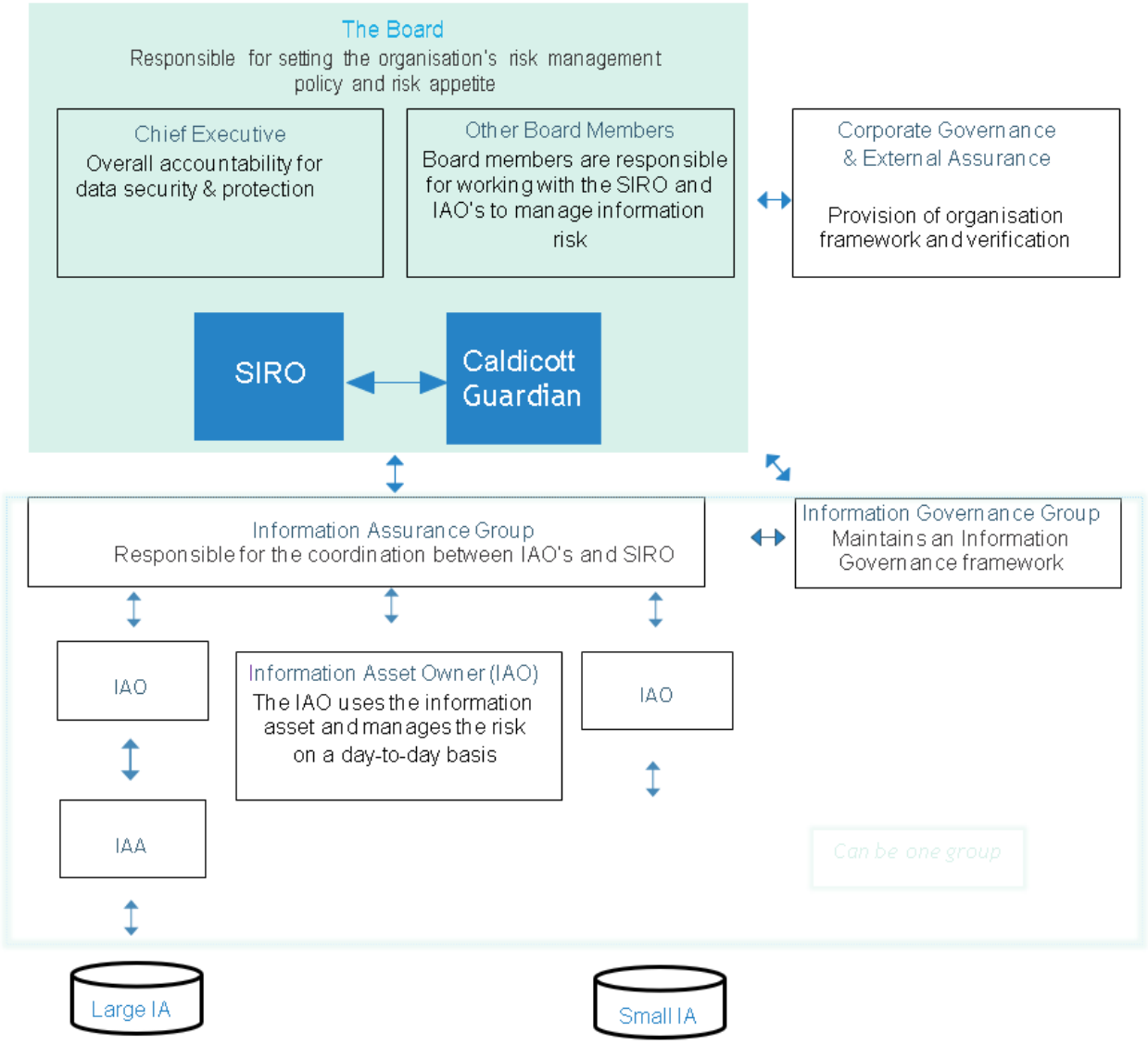
There is a clear understanding of what Personal Confidential Information is held.

Data Security Standard 2.1

SIRO, IAO, IAA, IA structure

If you have an existing information assurance structure in place that is based upon Information Asset Owners (IAO), Information Asset Administrators (IAA), Assets (IA) with assurance to the Senior Risk Information Owner (SIRO) this is compatible with the standard.

This may look something like the example below



*Adapted from the SIRO Manual from the National Archives

The NDG standards do not prescribe any predetermined structures other than that of SIRO approval. For the purposes of the standard, information asset and systems can be considered identical.

List of systems holding Personal Information

A list of systems should be maintained (as defined as those with 10% or more of staff / patient data) holding PCI (information that is personal and usually sensitive personal information that is held is subject to an obligation of confidentiality).

There is not a prescribed method of recording and maintaining this information, however this can be an existing information asset register, provided it meets the criteria (in definition and scope). The list should be reviewed periodically (at least annually).

The organisation has identified and catalogued personal and sensitive information it holds.

Data Security Standard 2.1.1

SIRO involvement

The SIRO should be involved informed of any issue when gathering and reviewing the systems / information assets list. The SIRO should also approve the list as being accurate.

When did your organisation last review the list of all systems/information assets holding or sharing personal information?

Data Security Standard 2.2.1

Data protection and security induction

When staff start with a new organisation, it is during their induction period when they can be at their most vulnerable. They may not understand the organisation's systems, policies and procedures, its cultures or norms.

The induction should help staff understand their obligations under the National Data Guardian's data security standards in their organisation. It should cover the following areas:

- the importance of data security in the care system
- the NDG data security standards, particularly the three standards relating to personal responsibility (standard 1, 2 and 3)
- the applicable laws (GDPR, FOI etc) knowing when and how to share and not to share
- understanding:
    - what social engineering is
    - safe use of social media and email
    - the dangers of malicious software
    - how to protect information
    - physical security.
- knowing how to spot and report data security breaches and incidents.

"The key issue is to ensure that staff are able to understand, and recognise the importance of, the basic principles in line with their role and are therefore adequately prepared to apply their knowledge to different scenarios in their daily working routines."

BMA

Your Data: Better Security, Better Choice, Better Care

Government Response

It is important that the messages are local and specific to your organisation and that they include local procedures and policies and where possible refer to examples of specific local incidents.

Is there a data protection and security induction in place for all new entrants to the organisation?

Data Security Standard 2.2.1

Delivery of the induction

There are no stringent guidelines on how the course is delivered, however it is important that it is effective and resonates with your audience. Some of the delivery methods you can consider are:

- a discrete separate event
- part of a wider employee induction
- face to face
- digital delivery (such as e-learning).

Staff scope

It is important that a record is kept of all staff at your organisation who have received appropriate training and when this is due for renewal. This also includes staff who work at, but not directly for, your organisation (such as contracted out service staff). The organisation either needs to verify that the training received by contracted staff is satisfactory, or ensure that those staff attend the organisation's induction.

Review

It is good practice to encourage staff to provide feedback on the induction itself in order improve it, but to also regularly review the content to ensure it is relevant and up to date.

Staff contracts

Appropriate clauses in staff contract should reference data security (confidentiality, integrity and availability). It is recognised that most contracts commonly focus on confidentiality clauses.

If you are managing third party personnel, you are likely be managing them through a contract as discussed in Data Security 10 Accountable suppliers.

Do all employment contracts contain data security requirements?

Data Security Standard 2.2.2

An improving picture

Feedback from staff awareness, feedback from inductions and lesson learnt from incidents should be used to improve staff awareness.

The results of Staff awareness surveys on staff's understanding of data security are reviewed to improve data security.

Data Security Standard 2.2.3

Appendix 1 -
Table of Data Security Level 2 Assertions

Assertion	Sub Assertion	Evidence
2.1 There is a clear understanding of what personal Confidential Information is held.	2.1.1	The organisation has identified and catalogued personal and sensitive information it holds.
	2.1.2	When did your organisation last review the list of all systems/information assets holding or sharing personal information?
2.2 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.	2.2.1	Is there a data protection and security induction in place for all new entrants to the organisation?
	2.2.2	Do all employment contracts contain data security requirements?
	2.2.3	The results of Staff awareness surveys on staff's understanding of data security are reviewed to improve data security.

Appendix 2 - Useful resources

Data and cyber security: protecting information and data in health and care: NHS Digital data security homepage

Links to news and guidance for organisations to support health and care to keep patient information and computer systems safe.

https://digital.nhs.uk/cyber-security

Guidance: National Cyber Security Centre

Expert, trusted, and independent guidance for UK industry, government departments, the critical national infrastructure and private SMEs. All our guidance is advisory in nature and is underpinned by our unique insights into cyber threats.

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

Guidance for supporting a systematic delivery of awareness programs and training that deliver security expertise as well helping to establish a security-conscious culture.

https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/user-education-and-awareness

Appendix 3 –
The National Data Guardian Reports

The NDG Report

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