NHS Digital

Data Security Standard 2

Staff responsibilities

The bigger picture and how the standard fits in

2021/22

Information and technology for better health and care

Contents

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.

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.

The NCSC has some resources detailed in the Appendix

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

Data Security Standard 2.1.1

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 contracts 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 2.1.2

An improving picture

Feedback from staff awareness, feedback from inductions and lessons learned 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 2.1.3

Appendix 1 -
Table of Data Security Level 2 Assertions

Assertion	Sub Assertion	Evidence
2.1 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.	2.1.1	Is there a data protection and security induction in place for all new entrants to the organisation?
	2.1.2	Do all employment contracts contain data security requirements?
	2.1.3	The results of Staff awareness surveys on staff's understanding of data security are reviewed to improve data security.

Appendix 2 - Useful resources

Guidance: Cyber and data security - NHS Digital

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

The resources introducewhy cyber security is important and how attacks happen, and then covers four key areas:

- defending yourself against phishing
- using strong passwords
- securing your devices
- reporting incidents ('if in doubt, call it out')

https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available

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