NHS England

# Data Security Standard 2

## Staff responsibilities

### The bigger picture and how the standard fits in

2023/24

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."*

It also explains that:

*"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."*

Please refer to further note on professional judgement, auditing and UK General Data Protection Regulation (UK GDPR).

https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/using-professional-judgement

# Staff inductions (2.1.1)

# 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.

Your organisation should have a data security and protection induction in place which helps staff to understand their obligations under the National Data Guardian's data security standards.

### The data security and protection inductions should cover:

- the importance of data security and protection in the health and care system
- the NDG data security standards, particularly the three standards relating to personal responsibility (standard 1, 2 and 3)
- the applicable laws (such as UK GDPR, freedom of information) and the common law duty of confidentiality, particularly knowing when and how to share and not to share
- knowing how to spot and report data security breaches and incidents and near misses

The induction should also contain specific sections on:

- what social engineering is
- safe use of social media and email
- the dangers of malicious software
- how to protect information
- physical security

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.

If you would like to see a practical example, the National Cyber Security Centre has produced an e-learning training package which can be integrated into your own organisation's training platform or learning management system (LMS). The introductory Data Security Level 1 Training and the new advanced e-learning on information sharing for frontline and administrative staff can also be accessed on ESR or hosted on your organisation's LMS. Speak to your HR team or LMS administrators if you would like to organise this.

### 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 separate event
- part of a wider employee day or programme
- face to face group sessions
- digital delivery (such as e-learning or webinars)

## 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 staff
- volunteers
- staff seconded into your organisation

The organisation either needs to verify that the training received by contracted staff by their parent organisation, such as an agency, is satisfactory or ensure that those staff attend the organisation’s induction.

## Review

It is good practice to encourage your staff to provide feedback on the induction they have received, both on the content and the delivery. This will allow you to refine it and make improvements.

You should also regularly review the content to ensure it is relevant and up to date.

# Employment contracts (2.2.1)

Your organisation's staff contracts should have appropriate clauses referencing data security and protection, with an emphasis on their duty to ensure the confidentiality, integrity and availability of health and care data. Most contracts commonly focus on confidentiality clauses, whilst overlooking the other important dimensions. Example clauses are available for organisations to adopt below.

> "By signing this contract, you confirm that you have read, understood and will comply with the organisation's data security and protection policies [or add your organisation's relevant policy or policies title(s) here], a copy of which is available at [add location] and agree to undertake mandatory information governance training, upon commencement of employment and on an annual basis thereafter.
>
> This clause applies to any information obtained during the course of your employment with the organisation and which is confidential in nature and of value to the organisation including but not limited to patient records and details, confidential information relating to organisation or business contracts, financial affairs, service or commercial contracts and information relating to confidential policies of the organisation.
>
> You may disclose confidential information as necessary for the purposes of carrying out your duties. However, you shall not, during your employment or at any time after its termination for any reason, use or disclose to any person or persons whatsoever (except the proper officers of the organisation or under the authority of the Board) any trade secrets, secret or confidential information and you shall use your best endeavours to prevent any such use or disclosure.
>
> Disclosure of confidential information, trade secrets or secret information other than in accordance with this clause may be detrimental to the business of this and other relevant organisations and may amount to gross misconduct.
>
> You will not obtain financial advantage, directly or indirectly, from a disclosure of confidential information acquired by you in the course of your employment. Your duty of non-disclosure continues after termination of employment.
>
> Nothing in this clause shall apply to information disclosed pursuant to any order of any court of competent jurisdiction or any information which, except through any breach of this or any other agreement by you, is in the public domain, is required by an appropriate regulatory authority or information disclosed for the purpose of making a protected disclosure within the meaning of Part IVA of the Employment Rights Act 1996."

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

# Appendix 1 – Useful resources

**Cyber and data security - NHS England**

Links to news and guidance for organisations to support health and care to keep patient and service user information and computer systems safe.
https://digital.nhs.uk/cyber

**Data security awareness programme: Health Education England**

Overview of the NHS England  training for Data Security Awareness Level 1, Level 2 and Level 3, as well as how to register as a user and access them.
https://www.e-lfh.org.uk/programmes/data-security-awareness/

**Advice and guidance: NCSC**

Expert, trusted, and independent guidance for UK industry, government departments, the critical national infrastructure and private small to medium sized enterprises (SMEs).
https://www.ncsc.gov.uk/section/advice-guidance/all-topics

**10 Steps to Cyber Security: NCSC**

Guidance on how organisations can protect themselves in cyberspace.
https://www.ncsc.gov.uk/collection/10-steps/engagement-and-training

**Top tips for staff: NCSC**

The resources introduce why cyber security is important and how attacks happen, and then covers 4 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/training/top-tips-for-staff-scorm-v2/scormcontent/index.html#/

# Appendix 2 – 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