NHS Digital

# Data Security Standard 3

## Staff Training

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

2020/21

Information and technology for better health and care

# Contents



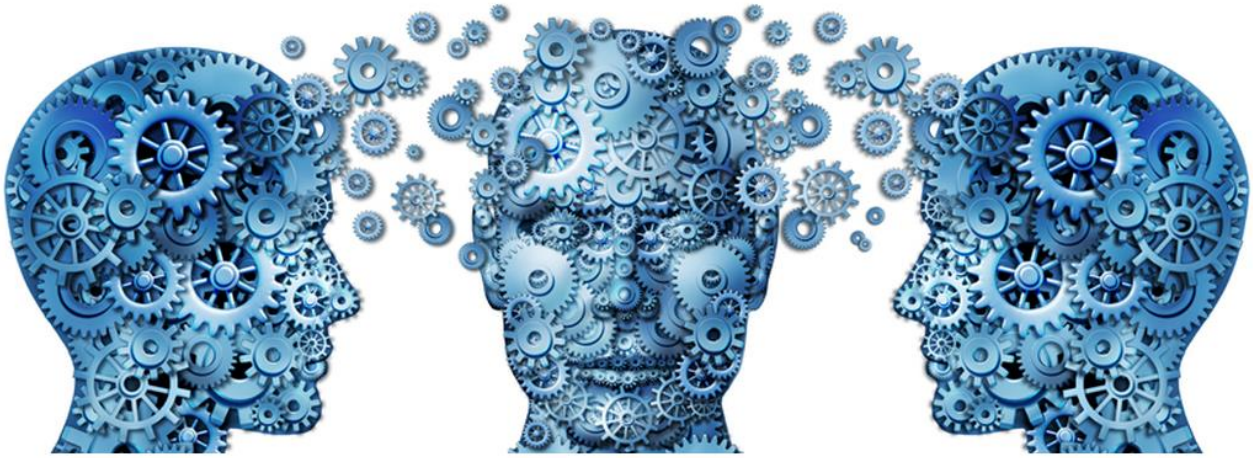
 

# Overview

## The NDG's review data standard 3 states that

*"All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit."*

Our fellow colleagues can be the greatest asset in spotting data security and protection issues and incidents. Unfortunately, our colleagues can also be exploited and inadvertently assist a cyber-attack. Our collective goal is to empower our colleagues with sufficient up to date knowledge allowing them insight and resilience.



# Using professional judgment

The DSPT guidance (audit framework and associated “big picture guides”) is not exhaustive. They will not cover every eventually and professional judgement will be required in how the standard is met and audited.

Both sets of guidance endeavour to be vendor agnostic. You may have an excellent vendor-supplied system which is not referred to in the guides. That is not to discount such a system, which should be implemented and audited on its merits.

The required standards have to be achievable to those whose digital maturity is still “developing”. As a consequence, some of the measures outlined could be seen as quite manual. This does not mean that more sophisticated measures cannot be implemented.

**At times the big picture guides may go further than the audit guides and vice versa. Only the most binary of assertions would lead to one answer. The divergence of guides is either following an implementation theme to the end or the next logical audit artifact**

When implementing or auditing please have regard to the intent of the evidence, assertions, standards and ultimately the whole 10 data security standards themselves. It is not the intention of the DSPT to create tick lists of items to be implemented and audited that bear little resemblance to actual practice.

# Training / Learning Needs Analysis

## Knowing your staff

An understanding of your current position in relation to your colleagues' data security and protection status is needed across the organisation.

This can be accomplished by a training (or learning) needs analysis.

An LNA (Learning Needs Analysis also known as a Training Needs Analysis or TNA) is a process which identifies current skills, knowledge and attitudes in relation to current and anticipated gaps in training and development needs. It may be carried out at an organisational level or in preparation for implementing new internal processes before the start of a training programme or course.

***NB The following details represent best practise, but you are free to use your TNA / LNA methodologies***.

*"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"*

**The British Medical Association**

Has an approved organisation wide data security and protection training needs analysis been completed in the last twelve months?

Data Security Standard 3.1.1

### An organisational level LNA:

- To identify overall data security and protection skills and knowledge gaps to help the organisation meet its future needs and developments

### What are the objectives of an LNA?

The LNA process will help the training team identify training requirements, plan the associated training activities and develop the training plan at an early stage of the training lifecycle. This will ensure that the training programme is:

- Clearly linked to organisational data security and protection objectives and expected outcomes
- Developed to address individual training requirements (knowledge and preferred learning style), and takes into account the training principles of the organisation
- Delivered with minimal impact on 'business as usual' by using methods appropriate to the needs of the training audiences, and within acceptable timeframes

## Benefits & Outcomes

There are many benefits to carrying out LNA. It:

- Provides information to help develop and design training solutions
- Helps to identify possible risks, constraints and dependencies that may affect the training
- Identifies resource requirements and restrictions
- Establishes pre-requisites for the training early in the process.

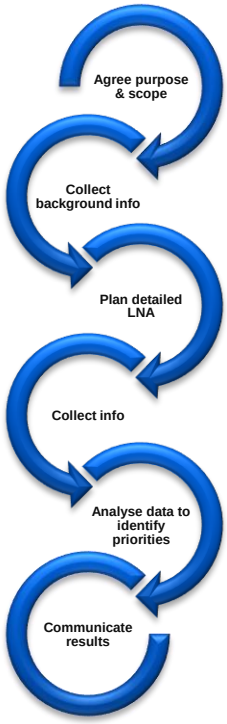
## LNA methods

LNA data collection methods can include several approaches: questionnaires, focus groups and interviews, job analysis, job evaluation and desktop reviews.

Methods which involve personal contact and active engagement with the individuals (e.g. interviews) are more time intensive but usually provide a better response rate and 'richer' data than more passive approaches, e.g. sending out a questionnaire.

## The LNA process

You need to plan the LNA process, which should include the following stages.




## Agree the purpose and scope of the LNA

- Confirm your Senior Information Risk Officer (SIRO) has overall responsibility for the data security and protection LNA and the timescales
- Agree with your SIRO and other stakeholders, what the LNA aims to achieve and at what level it needs to take place, i.e. across the organisation with a particular focus on data security and protection training
- Identify the scope of the LNA: who should be included and excluded e.g. maternity / paternity and long-term sick and secondees. Identify leaders and specialist staff.
- Establish what methods you will use (questionnaires/surveys, interviews or focus groups with staff or a mix of methods) and how they will be carried out.
- Is there a budget to support the LNA (think about resources needed, not just time)?
- Find out who your main contacts and/or champions are.
- Identify leaders and specialist staff.

## Collect background information

Find out if there is any existing data. For example:

- Has a similar LNA already been undertaken?
- What relevant information is available from Human Resources systems?
- Is there any relevant background information for the department or staff group you are targeting?

## Plan the detailed LNA

- Think about who will complete the questionnaires: you could ask managers or team leaders to do this on behalf of or as well as staff, but the information may not be as accurate.
- Check if there are any data protection and security issues around collecting and storing the data or how it will be used

## Collect information

- Design and pilot the questionnaire / survey
- Distribute and collect the completed questionnaire / survey
- Carry out the interviews or focus groups if applicable
- Store the information

## Analyse the data

- Quantitative analysis should be relatively straightforward. Analysing any qualitative data will take longer
- Identify important gaps in skills, knowledge and experience
- Identify the priority learning needs

## Communicate the results (LNA reporting)

- Write the LNA report
- Present the findings to your SIRO and other stakeholders
- Use the information for your training plan

## Integrate the information into the training plan

Once the LNA has been completed, you can use this information in the training plan to:

- Summarise important learning priorities
- Show how the identified gaps and needs will be met. e.g. through using a range of learning methods: digital learning, classroom courses, workshops and awareness sessions, workplace coaching, etc.
- Provide information about timescales, responsibilities and resources needed

## Analyse the data

Data needs to be analysed by people with the appropriate skills and experience and ideally by someone who has experience of carrying out LNAs. If you are not sure about analysing data, talk to your Information or Audit department.

If you use electronic data collection methods e.g. Survey tool or SharePoint, analysis of quantitative data is easier. However, you will need to analyse the free text and comments (qualitative data).

## LNA Report

The main deliverable of the LNA process will be in the form of an LNA report, which will allow you to confirm the approval of your training recommendations before proceeding to the next stage of the training cycle (Design and Development).
The extent and format of the LNA Report will vary, but typically such a report will contain reference to the following areas of information:

- **Executive Summary** – that can be used, if required, as a 'standalone' document, summarising the contents of the LNA Report
- **Introduction and aim** of the LNA Report
- **Methodology** – the LNA Approach adopted (e.g. methods for information gathering, audience sampling, etc.)
- **Skills gaps and needs** identified from the LNA
- **The recommended training solution**: include the scope and objectives of the proposed training programme based on LNA findings and competences required for the benefits to be realised. Show how the proposed training initiatives match the required training need
- **Train the Trainer and Post Training Support Programmes** – if required, to support the recommended training solution
- **Target training audiences** – detail the identified pre-requisite training requirements, skills and/or knowledge, staff level, numbers, timescales and timing of training roll-out
- **Training structure, content, methods and materials** – per audience group, where different as appropriate to the findings of the LNA
- **High Level Training Cost Breakdown** – based on LNA recommendations, subject to approval
- **Conclusion** - to support the main body of the LNA Report

## LNA approval

Before communicating the results to a wider audience this LNA needs SIRO approval.

Training Needs analysis has been approved by the SIRO or equivalent.

Data Security Standard 3.1.3

Communications before, during and following LNA work should be carefully planned and completed so that your findings do not come as a 'shock' to people.

Completing an LNA can also provide a good opportunity to raise awareness, begin to manage expectations, and build commitment to the training.

# National training for all Staff

All staff must complete appropriate data security training e.g. the national data security level 1 training. All staff must complete the data security level 1 test. The course is followed by a test, which can be re-taken unlimited times, but which must ultimately be passed. Staff are supported by their organisation in understanding data security and in passing the test. The training includes a number of realistic and relevant case studies.

Staff pass the data security and protection mandatory test

Data Security Standard 3.3

For clarity the term ‘staff’ includes all permanent and non-permanent staff that have access to personal confidential information.

The NDG data standards requirements relating to staff are listed below:

- 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.
- 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 complete appropriate annual data security training and pass a mandatory test, provided through the revised information governance toolkit.

Although the standard is ‘all staff’ it is recognised that a percentage of staff may be unavailable (i.e. due to maternity / paternity leave or long-term sickness), hence the 95% target.

95% of all staff including new starters, locums, temporary, students and staff contracted to work in the organisation have completed their annual Data Security Awareness Training (including passing a mandatory test). The 95% can be made up of staff completing the National E-Learning system or using local training systems or materials where this has been agreed as covering the learning objectives of the National E-Learning system (by your SIRO).

For more information on meeting this standard please see the Frequently Asked Questions: **https://www.dsptoolkit.nhs.uk/Help/30**

Have at least 95% of all staff, completed their annual Data Security awareness training in the period 1 April to 31 March?

Data Security Standard 3.2.1

## National training a minimum not a maximum

It should be recognised that national training provides the core learning messages from the National Data Guardian's review (appendix 3) and the government response. National training offers the minimum requirement and no matter how good national training is it can never capture all the unique local priorities and nuances.

Use of national training should be supplemented with local learning which is relevant to your organisation such as talks, blogs, posters, good / improvement news and emails.

## Specialist Staff Training

In addition to the training for all staff our colleagues with specialist roles should undertake specialist training in data security & protection. The type of roles covered:

- Information Governance Staff
- Information / Data / Cyber Security Staff
- IT / ICT / Informatics Staff
- Information Staff
- Data Quality Staff
- Staff with access to Personal Confidential Records

This list is not exhaustive and our colleagues with additional learning needs should be identified during the LNA.

The specialist level training covers more elements in data security and protection and to a greater depth.

Staff with specialist roles receive data security and protection training suitable to their role

Data Security Standard 3.4

## Data protection specialist training

The most recognised certification routes are from the British Computer Society (BCS) who offer two courses – a foundation level Foundation in Data Protection and a more advanced practitioner certificate in data protection.

According to the BCS, this training “provides an understanding of current UK data protection laws, including the EU General Data Protection Regulation (GDPR) and the UK Data Protection Bill, including how these are applied in practice and its importance for any organisation holding personal information.”

https://www.bcs.org/get-qualified/certifications-for-professionals/gdpr-and-data-protection-certifications/

## Clinical coding specialist training

Clinical coding has a set standard for the time frames and levels of training required.

The training given should use material that conforms to National Clinical Coding Standards. The Clinical Coding Standards Course which is of no less than 21 days duration for an Acute Trust coder and three days for a Mental Health Trust coder, must be attended within six months of commencing employment. Relevant staff must attend Clinical Coding Standards Refresher Course, or Mental Health Clinical Coding Standards Refresher Course training every three years thereafter. Further information can be found in the National Clinical Coding Training Handbook (see link below) and in the Clinical Coding Training section of the Publications & Resources page on Delen, the information sharing and collaboration platform for users of our Terminology and Classifications products. Here you can access up-to-date information, resources, educational materials and technical support relating to our core products.

It is imperative that all staff, including clinicians, who code using ICD-10 codes (and OPCS-4 codes where systems allow) are trained in the basics of clinical coding by attending the appropriate Clinical Coding Standards and Standards Refresher Courses as developed by the Terminology and Classifications Delivery Service.

The training may be provided by the organisation itself, as part of a local clinical coding consortium or by independent/commercial approved clinical coding trainers. The training must be delivered by a Terminology and Classifications Delivery Service Approved Clinical Coding Trainer in accordance with the Approved Trainer Requirements Framework and licence agreement using only materials developed by the Terminology and Classifications Delivery Service as well as other materials developed in accordance with National Clinical Coding Standards.

Furthermore, the organisation should provide a training and assessment framework which supports its clinical coders in gaining Accredited Clinical Coder (ACC) status by passing the National Clinical Coding Qualification (NCCQ) (UK). This is a marker of good practice and, in so doing, the organisation demonstrates due recognition of the professional status of clinical coding.

For more information, see the National Clinical Coding Training Handbook

https://hscic.kahootz.com/gf2.ti/f/762498/71837157.1/PDF/-/NationalClinicalCodingTrainingHandbook202021.pdf

## Data security specialist training and qualifications

There are number of vendors offering courses ranging from one day overview to a Masters cyber security degree. This guide gives an overview of the more commonly recognised training offerings.

If you are a smaller organisation a course such as the Open University (OU) Introduction to cyber security may be appropriate.

https://www.futurelearn.com/courses/introduction-to-cyber-security

- ISC2 (International Information Systems Security Certification Consortium)
  CISSP (Certified Information Systems Security Professional)

Probably the most commonly recognised is the ISC2 CISSP. According to ISC2 *"The CISSP is an objective measure of excellence. It's the most globally recognised standard of achievement in the industry. And this cybersecurity certification was the first information security credential to meet the strict conditions of ISO/IEC Standard 17024."*

- ISC2 SSCP (Systems Security Certified Practitioner)

SSCP is a foundation certification and could be considered a precursor towards CISSP. According to ISC2 *"This well-known, global IT security certification offers instant credibility. And it's an excellent way to expand your cybersecurity knowledge — particularly if you're in a hands-on, operational IT role or you're building a foundation in information security."*

https://www.isc2.org/

- ISACA (Information Systems Audit and Control Association)
  CISM (Certified Information Security Manager)

ISACA general information security management is the Certified Information Security Manager (CISM). According to ISACA *"The uniquely management-focused CISM certification promotes international security practices and recognizes the individual who manages, designs, and oversees and assesses an enterprise's information security."*

http://www.isaca.org/Certification/CISM-Certified-Information-SecurityManager/Pages/default.aspx

- BCS Information Security Management Principles

According to the BCS *"This certification provides candidates with good knowledge and understanding of the wide range of subject areas that make up information security management. This includes cyber security, risk management, vulnerabilities in social media, legislation, security standards (ISO 27001), business continuity and cloud computing."*

https://certifications.bcs.org/category/15733

- EC-Council Certified Chief Information Officer C|CISO

According to the EC-Council *"Each segment of the program was developed with the aspiring CISO in mind and looks to transfer the knowledge of seasoned professionals to the next generation in the areas that are most critical in the development and maintenance of a successful information security program."*

https://cert.eccouncil.org/certified-chief-information-security-officer.html

- Sans MGT512: Security Leadership Essentials for Managers

According to Sans *"This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security."*

https://uk.sans.org/course/security-leadership-essentials-managers-knowledge-compression

The organisation has appropriately qualified technical cyber security specialist staff and/or service.

Data Security Standard 3.3.2

## The Cyber Associates Network

The Cyber Associates Network is aimed at professionals with responsibility for or an interest in cyber security, including board members, IT leads, security professionals and cyber tech experts. Membership is free and offers a range of benefits.

You should have a nominated member of the Cyber Associates Network for your organisation.

For more information and to register:

https://digital.nhs.uk/services/data-security-centre/cyber-associates-network

The organisation has nominated a member of the Cyber Associates Network.

Data Security Standard 3.3.3

## Leaders and board members

The National Data Guardian's review (appendix 3) identified the tremendous benefit to organisation who have actively engaged leaders, especially the SIRO and other board members.

Leaders and board members receive suitable data protection and security training

Data Security Standard 3.4

Have your SIRO and Caldicott Guardian received appropriate data security and protection training?

Data Security Standard 3.4.1

Learning opportunities for leaders and board members should be appropriate to the seniority of the leaders and the accountability they hold. Uptake is measured for SIROs and board members and forms part of this standard.

# Appendix 1 -
# Table of Data Security Level 3 Assertions

| Assertion | Evidence | Evidence |
|---|---|---|
| **3.1 There has been an assessment of data security and protection training needs across the organisation** | 3.1.1 | Has an approved organisation wide data security and protection training needs analysis been completed in the last twelve months? |
| **3.2 Staff pass the data security and protection mandatory test** | 3.2.1 | Have at least 95% of all staff, completed their annual Data Security awareness training in the period 1 April to 31 March? |
| | 3.2.2 | What is the average mark of staff completing the Data Security Awareness Training? |
| **3.3 Staff with specialist roles receive data security and protection training suitable to their role** | 3.3.1 | Provide details of any specialist data security and protection training undertaken. |
| | 3.3.2 | The organisation has appropriately qualified technical cyber security specialist staff and/or service. |
| | 3.3.3 | The organisation has nominated a member of the Cyber Associates Network. |
| **3.4 Leaders and board members receive suitable data protection and security training** | 3.4.1 | Have your SIRO and Caldicott Guardian received appropriate data security and protection training? |
| | 3.4.2 | What percentage of Board Members have completed appropriate data security and protection Training? |

# Appendix 2 - Useful resources

**NHS IT Training Professionals forum on NHS Networks.**

For more details on how to join this forum, please contact the Training Quality Improvement Team:

tqi@nhs.net

**NHS Digital Training Quality Improvement**

Use the education and training standards online benchmarking application (ESOBA) to self-assess your training service against the national standards. You can also upload supporting evidence and calculate your achievement level.

http://content.digital.nhs.uk/article/4917/Standard-2---Planning-and-Learning-Needs-Analysis

**Chartered Institute of Personnel and Development**

The professional body for experts in people at work. Championing better work and working lives by setting professional standards for HR and people development, as well as driving positive change in the world of work. They have about training needs on their website (Please note that some articles have restricted access for members only):

www.cipd.co.uk/hr-resources/factsheets/identifying-learning-talent-development-needs.aspx

**E learning for Healthcare**

Health Education England works across England to provide high quality education and training for a better health and healthcare workforce. They host the data security training:

https://nhsdigital.e-lfh.org.uk/

# 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

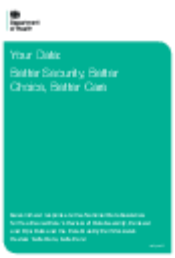
### The Government Response

‘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