NHS England

Data Security Standard 3

Staff Training

The bigger picture and how the standard fits in

2023/24

Information and technology for better health and care

Contents

Overview

Staff have appropriate understanding of information governance and cyber security, with an effective range of approaches taken to training and awareness.

“Our colleagues are our best defence against patient harm from cyber-attacks. Appropriate training helps in avoiding disruption to patient care and avoiding patient harm. Organisations now have the flexibility to determine how best to interpret their responsibilities to respect people’s confidentiality and manage cyber security risk and ultimately enhance patient safety.”

Phil Huggins

National Chief Information Security Officer for Health and Social Care

Please refer to further note on professional judgement, auditing and GDPR.

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

What's changed for 2023/24?

Until July 2023, the DSPT required that you train at least 95% of your staff using the national Data Security Awareness Level 1 e-learning or a local equivalent.

This has changed for 2023/24. You now need to ensure that all your staff have an **'appropriate understanding of information governance and cyber security'.**

This means that you will have more flexibility to set local training requirements that are appropriate to different staff roles, and to adopt a range of different methods to deliver that training. Your approach will need to be proportionate to the size and type of your organisation.

The new DSPT training requirement consists of three parts, for which guidance follows below:

- **Training needs analysis**
  You will need to analyse staff training needs to decide what 'appropriate understanding' means for your staff. This is likely to vary between roles.

- **Delivery of training and awareness activities**
  You will need to deliver the training and awareness activities that you decide will maintain the appropriate level of understanding across the different staff roles.

- **Evaluation**
  You will need to evaluate the effectiveness of your approach to ensure that you have met the underlying outcome of appropriate understanding.

Training needs analysis (3.1.1)

“Training and awareness activities form part of organisational mandatory training requirements, with a training and awareness needs analysis (covering all staff roles) that is formally endorsed and resourced by senior leadership.”

Before you deliver any training, you should understand what training and awareness is needed to ensure that your staff have an appropriate level of understanding.

All staff working in a health and care organisation need some understanding of information governance (IG) and cyber security. The level will vary depending on the staff member’s role, for example:

- a staff member with routine access to employee or confidential health and care information needs to understand how to protect and handle it appropriately to ensure it is accurate and available when needed.
- researchers and senior health professionals need a more advanced understanding of what they can and cannot lawfully do with confidential health and care information.
- a staff member using a digital device such as a PC, tablet or smartphone needs to be aware of their responsibilities to protect information from cyber risks. This includes staff working in areas such as facilities and estates.
- a staff member who unintentionally comes across confidential information, for example by overhearing a conversation or seeing sensitive details displayed in a work area, needs to understand how to respond appropriately.
- staff members whose roles require additional data security and protection training such as information governance staff or data protection officers.

The process of deciding the level of understanding that different staff groups need to have, and the training that is best suited to achieving it, is known as a training needs analysis (TNA). You can use any appropriate method for your analysis and record it in any format you choose.

Conducting a TNA allows your organisation to:

- assess the level of training appropriate for each staff group
- plan resources needed to deliver training
- deliver role-specific training
- identify and address potential gaps in the delivery of training

TNAs are iterative – as your organisation completes one cycle of training, the TNA should be reviewed and updated to reflect new national requirements, refinements in the delivery of training based on staff feedback, or changes within your organisation that impact the TNA.

Once completed and approved, the TNA should be uploaded as part of your response to 3.1.1.

View an example TNA template for a fictional organisation. You can use one of these template TNAs or another template.

Frequency of training

As part of the TNA, you should consider the frequency of training appropriate for each role, for example:

- on joining your organisation and annually thereafter, or
- different refresher intervals for different roles.

You are free to decide what is appropriate, provided it meets the outcome of staff having and retaining the necessary understanding for their role.

Appropriate resourcing and approval

Your TNA should be formally endorsed by your board or equivalent senior leadership and resourced appropriately, so that it is realistic. You should include evidence of this as part of your response to 3.1.1.

Delivery of training and awareness activities (3.1.2)

“Your organisation’s defined training and awareness activities are implemented for all staff.”

Training and awareness-raising activities can be delivered in a variety of ways, and you are free to decide which methods to use for different staff groups.

It is good practice to use a range of training approaches, and this usually results in better participation and comprehension. Some people respond well to e-learning; others may benefit more from face-to-face training. See for example the good practice guidance on training and awareness published by the ICO and NCSC.

Both formal training and informal awareness-raising methods have their place in delivering the different levels of understanding required.

Formal training is more structured and measurable, and can be useful to ensure specific topics are covered across a group, or to deliver more complex or compliance-based content. For example, you might decide to use e-learning to provide basic knowledge to all staff, with additional training in different forms to meet the specific needs of different staff groups.

Informal methods can be very helpful to raise awareness across the organisation or for specific staff groups. Alternatively, you might decide that formal training isn’t appropriate for staff that need a less advanced level of knowledge, and therefore maintain their awareness through less formal methods.

Your programme can take into account previous training that individuals may have received in your organisation or elsewhere, and the current level of awareness in different groups in your organisation. Interviews with a small representative sample of each staff group can help you gain an understanding of this.

Monitor and record your activities

You will need to monitor and record your training and awareness activities to give assurance to your board and auditors that you are delivering them in accordance with your training needs analysis and reaching all relevant staff.

Formal training approaches

Formal training is delivered in a systematic, intentional way. It can occur in a face-to-face setting or through an online learning platform. This training is structured and more easily measurable, and can be useful for detailed training or to ensure coverage of specific topics. Here are some examples of formal training approaches that can contribute to the required outcomes:

- in-house face-to-face training (with national or local training material – such as an induction presentation)
- e-learning modules (such as the national Data Security Awareness module)

- external conferences or courses – attending relevant cyber or IG events (with Continuous Professional Development (CPD) points or certificate of attendance)
- course syllabus with modules covering data protection and confidentiality which have been completed by newly qualified frontline staff such as a nurse or social worker
- relevant qualifications obtained by staff in specialist roles

Training for senior and specialist staff

It is important that your plans account for the specific training required for the following 3 staff groups:

1. Senior leadership roles – this includes:
    - Senior Information Risk Owners (SIROs)
    - Caldicott Guardians
    - other board members

2. Specialist staff - ‘specialist staff’ in this context refers to those whose roles include particular responsibility for handling or protecting information, and therefore require advanced training in data security and protection, such as:
    - information governance staff
    - cyber security and IT staff

3. Clinical coding roles

Leaders and board members

Having leaders who are actively engaged in data security and protection brings tremendous benefits to organisations.

SIROs, Caldicott Guardians and other members of the board should receive specialist training that is relevant to their role as soon as they are appointed, as well as regular refresher training, in line with your TNA. Your organisation may choose to deliver bespoke training through your own teams or you may use a third-party training provider. It is important that training programmes for SIROs, Caldicott Guardians and board members (including both executive and non-executive roles) cover both cyber security and IG.

Learning opportunities for leaders and board members should be appropriate to the seniority of the leaders and the accountability they hold. SIROs in NHS trusts and CSUs can access cyber security training free of charge through NHS England. Caldicott Guardians can take various routes towards specialist training: free training is available via e-learning for healthcare and further information is available at the Caldicott Guardian Council website.

Clinical coding staff

Clinical coding has a set standard for the time frames and levels of training required. The training given must use material that conforms to National Clinical Coding Standards and applies to both classroom-based and online delivery formats. For further information see Appendix 1 & 2 of this document.

Awareness raising activities

These activities will support continued awareness and can be used to deliver highlights and time-limited themes or signpost to more detailed training. They will need to be used in combination with more formal methods to meet all of the required outcomes for your organisation. Useful content and graphics to support these activities are available as part of the Keep I.T. Confidential campaign.

Here are examples of activities you can run to raise awareness in the workplace:

Intranet pages

Normally available to all staff who use a computer, and can be updated regularly. You can include dedicated cyber security and IG information pages prominently on your staff intranet.

Staff newsletters

These can be made available to all staff via email and intranet and printed off and put on noticeboards for staff that do not use IT equipment. They can include regular updates regarding IG and cyber security news, tips and tricks, as well as learning opportunities.

All staff events

Speakers from your IG and cyber security teams can present and answer questions. Presentations can be made at team, department or specialty level, with content tailored to the audience.

Lunch and learn sessions

Run a series of lunch and learn topic-based sessions either face-to-face, remotely, or a combination of the two. The series could cover topics such as password protection; protecting personal and confidential data; sharing information; email phishing; tailgating; physical offline security; social engineering; unlocked screens; and privacy best practice.

Drop-in clinics

Run weekly or fortnightly drop-in clinics for staff to attend with their specific IG and cyber security questions. This method can be useful to identify potential incidents or risks, develop 1:1 knowledge, and signpost staff to appropriate training.

Shadowing opportunities

Offer shadowing access to more experienced staff to showcase what good cyber and IG practice looks like in everyday work.

Videos

Key IG and cyber staff can record pieces to camera to help inform and educate staff. These short, educational videos can then be posted to your staff intranet.

Staff awards

Share examples of staff and teams who are championing good IG and cyber behaviours. Consider nominating them in your staff awards scheme to provide recognition and positive reinforcement of those behaviours.

Examples of regulatory action

Use examples where regulators such as the Information Commissioner's Office (ICO) has taken action against staff working in health and care – to highlight that data protection and cyber security is taken seriously.

Case studies

Post to your staff intranet case studies or blog posts of queries reported to IG and IT/cyber teams that prevented an incident occurring.

Keep I.T. confidential campaign

Use the free resources from the Keep I.T. confidential campaign to promote good IG and cyber security around your setting.

- Print and display the posters around your site
- Share material on your social media channels
- Run the digital banners on your intranet site
- Promote training through email signature banners
- Use the pop-up banners for events and physical spaces
- Install screen savers on staff computers

Evaluation (3.1.3)

“Provide details of how you evaluate your training and awareness activities.”

By evaluating your training and awareness activities, you will understand whether the training needs set out in your analysis have been met, and whether you have achieved the outcome of staff having appropriate understanding of IG and cyber security.

There are a variety of ways you could seek to evaluate the effectiveness of the training methods you have implemented in your organisation.

Models of evaluation

The Chartered Institute of Personnel and Development provides more detailed guidance on methods that can be used in evaluation. The Kirkpatrick model is the most prevalent framework for evaluating learning, and consists of four evaluation levels: reaction, learning, behaviour and results.

For example, the ‘reaction’ level can be assessed with questionnaires at the end of a training session. Determining whether staff then retain the knowledge and skills from the training requires more in-depth evaluation.

Your organisation should regularly monitor the effectiveness of your training methods. If your chosen methods are not producing the anticipated results, you will need to review why, and make the necessary changes – either to your training material or methods – to increase compliance. This should also result in an updated TNA to reflect the new approach.

A few examples are provided below:

Evaluation technique	Description	Time needed	Number of respondents
Post training questionnaire	Participants are asked to complete a short survey at the end of the training / intervention to assess their reaction	Low	Medium / high
Survey	Undertaking regular surveys of a random sample of staff both before and after interventions, can demonstrate change over time	Low	High
Focus groups	Running focus groups with a cross section of staff can allow for more detailed feedback on the effectiveness of an intervention	Medium	Medium
Interviews	One to one interviews allow for more in-depth questioning	High	Low

Suspicious emails reported to IT	IT departments may be able to provide data on the number of suspicious emails reported, or other relevant metrics which could demonstrate a shift in cyber awareness	Low	High
Evaluation of IG and cyber queries	Number of queries reported that would or could have led to incidents if no advice had been sought.	Medium	Medium
Evaluation of incidents reported internally	Review of incidents reported by different staff groups that have inadequate staff awareness as a contributing factor	Medium	Medium
Audits	Independent evaluation of the training activities in place and their respective outcomes	High	Medium
Spot checks	Random checks on individual activities linked to training	Medium	Low
Number of incidents reported to the ICO	IG teams should hold a record of any incidents reported to the ICO	Low	Low

Audit

The DSPT audit guidance will cover training with a focus on the governance of the TNA approvals; whether the proposed approach is proportionate to the size and type of your organisation; and evidence of implementation.

Culture (3.2)

Outcome: "Your organisation engages proactively and widely to improve information governance and cyber security, and has an open and just culture for information incidents."

The culture of an organisation starts with its most senior leaders. The behaviours that they demonstrate as role models, and support and encourage staff to adopt, can have a huge influence on an organisation's culture.

If senior leaders regularly talk about IG and cyber security, support local campaigns and improvement initiatives, and address incidents and problems openly and consistently, a positive culture will emerge. Staff will feel able to report incidents and speak openly about concerns and will work together across the organisation to improve practices. They will make an extra effort to 'do the right thing' and follow organisational policies and procedures, knowing that they will be listened to fairly if they have concerns about what those policies require of them.

If senior leaders treat IG and cyber security as inconveniences, take no interest in improvement work, and assign blame in incidents, a negative culture will emerge. Staff will feel unable to speak openly, and problems are likely to be covered up. They will know that policies and procedures are not taken seriously, so will ignore or work around them.

Culture is harder to change than a policy or procedure but has a greater effect. A negative culture easily undermines good policies, and a robust procedure is irrelevant if nobody follows it. Similarly, the knowledge and skills learned in training will be of no value if your organisational culture does not enable staff to use them in their daily roles.

Board prioritisation (3.2.1)

"Information governance and cyber security matters are prioritised by the board or equivalent senior leaders."

Prioritisation means that IG and cyber security are given proportionate time and support at board level, not that they are prioritised above everything else. This is likely to be led by the Senior Information Risk Owner (SIRO) or other board member(s) with specific responsibility for cyber and IG but is only effective if it involves the whole board. This could, for example, be with regular discussion of risks, and agreements to provide resources or funding to support improvement and awareness initiatives.

Senior leaders being visibly present across the organisation to discuss IG and cyber matters and promote improvement or awareness campaigns will help to demonstrate to staff that your organisation takes it seriously. Specialist leads such as the SIRO and Caldicott Guardian likely already do this because of their roles, but this will be even more effective if staff across the organisation can see their own professions and departments leading by example. Ensuring that other senior leaders such as the medical, nursing and finance directors are actively engaged in leading discussions about cyber and IG, and supporting improvement initiatives, will mean that staff can directly relate it to their own roles.

Responding to concerns (3.2.2)

“Actions are taken openly and consistently in response to concerns.”

Incidents are sometimes seen as a ‘bad thing’ – nobody wants things to go wrong, and more incident reports can be perceived to mean that more things have gone wrong. But no organisation is perfect and there is always a risk where data is used; things will go wrong at some point, and what matters then is how you deal with it.

Incident reporting is also a sign that staff understand their responsibilities, and want to report a problem to give the organisation an opportunity to do better in future – to improve practices for staff, and improve outcomes for individuals. You may also have concerns raised directly by patients or members of the public.

If your organisation habitually responds fairly and transparently to incidents and concerns that are raised, people are more likely to continue raising them, and you will have more opportunity to improve.

You can achieve this by adopting a ‘just culture’ – treating staff involved in an incident in a consistent, constructive and fair way. In a just culture, people who have caused incidents deliberately or through negligence or recklessness should be held to account, but honest mistakes are not punished. By looking critically at the processes that led to incidents, you can address underlying issues and make improvements without assigning blame.

Further guidance on just culture in an IG and cyber security context will be published by NHS England.

Staff engagement (3.2.3)

“Your information governance and cyber security programme is informed by wide and representative engagement with staff.”

The programmes managing IG and cyber security, and ongoing work, will already reflect the priorities set by the board – if only at a basic level reflecting the available resources.

The programme should also be informed by engagement with staff in order to meet operational needs. This can be as simple as ensuring that your steering groups have representative membership, so that each department has a voice in the programme – and so that those members will then champion IG and cyber security within their departments.

Other initiatives may involve staff across the organisation more directly, such as reviewing and updating your information assets and flows register.

If your organisation has a positive culture about IG and cyber security, staff will want to be involved, and are more likely to take the initiative and create improvements without being directed. Their experience and expertise in their own areas, and their joint ownership of the activities, will help build a strong and effective programme.

Appendix 1 - Training for clinical coding

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

Only those already employed as clinical coders within an NHS trust or an independent sector treatment centre, or clinical coders who have previously passed the Clinical Coding Standards Course (CCSC) and are working as contract clinical coders, are entitled to attend national clinical coding training courses. Contract clinical coders will not necessarily be in employment at the time of attendance on a course such as the Clinical Coding Standards Refresher Course (CCSRC).

The training given must use material that conforms to National Clinical Coding Standards and applies to both classroom-based and online delivery formats. The CCSC is delivered in no less than 21 days duration for an acute trust coder and 3 days for a mental health trust coder.

Attendance on the CCSC must start within 6 months of commencing employment as a clinical coder in an NHS trust or other organisation responsible for coding inpatient NHS activity. Relevant staff must attend CCSRC, or Mental Health Clinical Coding Standards Refresher Course training, every 3 years thereafter [1]

Further information can be found in the National Clinical Coding Training Handbook and in the Clinical Coding Training section of the Publications and 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 essential 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 an NHS England 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.

1 This is a Data Security Protection Toolkit requirement and is not linked to a clinical coder's accredited clinical coder (ACC) status - a clinical coder will not lose their ACC status as a result of not attending a CCSRC within the required timeframe.

NHS England - National Clinical Coding Training Handbook

Provide the necessary training in the general and specialist knowledge and skills required to use the national clinical coding standards including an outline of the mandatory national clinical coding standards course (CCSC), Clinical Coding Standards Refresher Course (CCRSC), Mental Health Clinical Coding Standards Course (MHCCSC), Mental Health Clinical Coding Standards Refresher Course (MHCCSRC), and the NCCQ (UK) Revision Programme.

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

National Clinical Coding Training – Interactive Presentation 2023-24

This is an abridged version of the National Clinical Coding Handbook, containing all the basic information regarding the various national clinical coding training courses.

https://nhsengland.kahootz.com/gf2.ti/f/762498/159654213.1/PDF/-/CCTPHandbook%202023-24v8.0.pdf

NHS England - Publications and Resources page on Delen

Contains a Clinical Coding training section 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.

https://nhsengland.kahootz.com/t_c_home/groupHome

Appendix 2 - Useful Resources Data Security Standard 3

Training Needs Analysis Template

https://www.dsptoolkit.nhs.uk/News/Attachment/726

NHS England Quality Improvement Training

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.

https://digital.nhs.uk/services/training-quality-improvement

Cyber Associates Network (CAN)

CAN members benefit from enhanced knowledge-sharing, professional development and networking with peers in health and care.

https://digital.nhs.uk/cyber-and-data-security/about-us/cyber-associates-network

Specialist training for SIROs: NHS England

A free cyber security training course offered by NHS England for Senior Information Risk Owners (SIROs) working in NHS trusts and Commissioning Support Units (CSUs).

https://digital.nhs.uk/cyber-and-data-security/training/specialist-training-for-siros

The role of the Caldicott Guardian

E-learning for Caldicott Guardians, and those with an interest in finding out more about the role Caldicott Guardians play in keeping people's health and social care data safe, and ensuring it is used appropriately.

https://www.e-lfh.org.uk/programmes/the-role-of-the-caldicott-guardian/

Data Security Awareness - Level 1

Staff can access this free Data Security Awareness Level 1 session produced by NHS England for an introduction to data security and cyber awareness.

https://portal.e-lfh.org.uk/Component/Details/544107

Information sharing – advanced module for frontline staff

Scenario-based training produced by NHS England which staff can access for free to help them understand the principles behind information sharing and how to apply them in practice.

https://www.e-lfh.org.uk/programmes/information-sharing/

Immersive Labs online cyber security e-learning

NHS England is offering health and care colleagues free user licences for Immersive Labs, an innovative cyber security learning platform**.**

Immersive Labs is a gamified learning environment that helps users develop their skills in cyber security. With something to suit all roles from administration to technical architecture, information governance to cyber analysis – it offers customised training all under one platform.

You can claim Continuing Professional Education (CPE) credits by completing challenges on the Immersive Labs platform.

Licences are available to everyone working for a health and care organisation. Complete the request form to register.

https://digital.nhs.uk/cyber-and-data-security/training/immersive-labs-online-cyber-security-e-learning

High quality education and training for a better health and healthcare workforce.

https://portal.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