Training and skills development for the care sector

Published by the Institute of Public Care in collaboration with the Better Security, Better Care programme

Published July 2022

Training and skills development for the care sector

1 Introduction

Better Security, Better Care is a national programme to improve data and cyber security in the adult social care provider sector. The programme supports the sector with resources and assistance to help care providers complete the Data Security and Protection Toolkit (DSPT). Most care providers are small and medium sized enterprises (SME) who often do not have access to data and digital experts and do not have internal learning and development capacity. Sourcing and regularly delivering suitable training on data security and protection, and cyber security, to frontline staff - and for those with specialist roles or responsibility for data protection - is one of the key challenges for SME care providers in meeting legislative requirements.

The Institute of Public Care (IPC) at Oxford Brookes University was asked to identify the data security and protection training needs of SME care providers, including how well current provision meets those needs, and how the training market could be developed. We undertook a programme of research to identify what DSPT compliant training looks like, reviewed existing free training resources, developed a skills assessment for frontline staff, and explored how the Caldicott Guardian role is represented in the sector. As well as desk research, we interviewed and met with care providers, Better Security, Better Care Local Support Organisations, Caldicott Guardians and Data Protection Officers working in the sector, the UK Caldicott Guardian Council (UKCGC), and a range of sector stakeholders such as Skills for Care, NHS Transformation Directorate, Digital Social Care and the Local Government Association. This report was presented to the Better Security, Better Care board in April 2022.

2 Minimum standard of training to comply with the DSPT

2.1 What is the requirement for annual training for staff?

Evidence item 3.2.1 asks “Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and protection, and cyber security, since 1st July 2021?”

The National Data Guardian’s Data Security Standard (see 2021/22 Data Security Standard 3: Staff Training at https://www.dsptoolkit.nhs.uk/Help/23) states that the minimum requirements are:

- “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."

Appropriate data security training is defined as the national Health Education England (HEE) / NHS Digital course Data Security Awareness Training (DSA) level 1, hosted by elearning for healthcare, which includes passing the course's mandatory assessment that has a pass mark of 80%.

The DSA course was revised in 2020 to meet the learning outcomes for Information Governance in the UK Core Skills Training Framework for healthcare services. The current key learning outcomes for the national NHS training, and hence the minimum standard of training that any training materials must cover to be compliant with evidence item 3.2.1, are that the learner will:

1. understand the principles of Information Governance and the importance of data security in health and care
2. understand the different types and value of information
3. understand the principles of data security, including how to ensure the confidentiality, integrity and availability of data
4. be aware of threats to data security and know how to avoid them, including:
   i. Social engineering i.e. the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes
   ii. Using social media safely
   iii. Using email safely
   iv. Malicious software
   v. How to protect information
   vi. Physical security
5. be able to identify data breaches and incidents and know what to report
6. understand fundamentals of data protection and the General Data Protection Regulations (GDPR)
7. understand the Caldicott Principles and be able to provide a confidential service to patients and service users
8. understand the responsibilities of healthcare organisations under the Freedom of Information Act 2000
9. understand individual responsibilities in responding to a Freedom of Information request

Further clarification from the UK Caldicott Guardian Council has confirmed that organisations can use local training systems or materials, instead of the national NHS eLearning course, where this has been agreed as covering the learning objectives of the national system and includes an assessment: "Locally produced training will be reported to and signed off by the local organisation's [Senior Information Risk Owner] SIRO or Caldicott Guardian and all staff completing the training will have to achieve the 80% pass mark."

2.2 What is the requirement for training for specialist roles?

On **toolkit registration** (and again on publication) care providers are asked to “enter key role details” for Caldicott Guardian, SIRO, IG lead, and Data Protection Officer.

Evidence item 1.1.5 asks “Who has responsibility for data security and protection and how has this responsibility been formally assigned?

Evidence item 3.4.1 asks “Have the people with responsibility for data security and protection received training suitable for their role?”

Data security and protection responsibilities for social care organisations are explored in the Digital Social Care resource Data Security and Protection Responsibilities, which defines a Data Security and Protection Lead (DSPL) as the person who takes overall senior responsibility for data security and protection in small social care provider organisations (as per evidence item 1.1.5).

There are no minimum NDG standards for training for Data Security and Protection Leads, or the other specialist roles asked for at toolkit registration, beyond the requirements for training all staff. The Digital Social Care resource recommends that the Data Security and Protection Lead completes the national NHS eLearning course Data Security Awareness or equivalent.

2.3 What is the requirement for induction?

Evidence item 2.1.1 asks “Does your organisation have an induction process that covers data security and protection, and cyber security?”

The National Data Guardian’s Data Security Standard (see 2021/22 Data Security Standard 2: Staff Responsibilities at https://www.dsptoolkit.nhs.uk/Help/23) states that the minimum requirements are:

“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:

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

3 Analysis of existing training resources

3.1 Resources for annual training of staff

There are an array of information governance / data protection commercial training courses available to purchase. Some commercial courses are designed for the health and care sector, but many are not suitable for smaller adult social care providers. Given the likely budgets of SME care providers, we focussed on reputable training that is freely available.

We reviewed existing, free to the sector training resources from nationally recognised bodies and analysed gaps between these current training resources and the minimum standards identified above. Nationally recognised bodies included Skills for Care, Digital Social Care, the National Cyber Security Centre, the Open University, BT and Barclays. Whilst the Information Commissioner's Office (ICO) and Get Safe Online are also nationally recognised bodies, with extensive information and advice about data security and protection, they do not provide training resources. Our review of national training resources is given below and a summary gap analysis against the key learning outcomes needed to be compliant with evidence item 3.2.1 is shown in the table below.

3.1.1 HEE / NHS Digital Data Security Awareness Training level 1

Anyone in the UK can register for free and access the national NHS training via the following link: https://portal.e-lfh.org.uk/Register. However, this is not made clear here https://www.e-lfh.org.uk/programmes/data-security-awareness/ and the information provided on how to access the course is not straightforward.

Organisations can register a large number of employees (in one go) and request administration rights for reporting purposes. Care providers can also obtain a SCORM (Sharable Content Object Reference Model) version so that they can host the course on their own learning management system if they have one.

The elearning course has an introduction plus seven sections / modules and is followed by an assessment, which can be re-taken unlimited times, but which must ultimately be passed. Staff can take the assessment without undertaking the training first as a separate assessment module has been created so that it is possible for the learner to complete the assessment without the need to complete repeated annual training if they have the requisite knowledge.

Social care organisations report that they find it difficult to gain access to this training course *"it was a faff to get on to! People might have given up if they'd had to go through the hoops I had to to get onto it"*. The language and examples are NHS-focused, it does not address the key risks for social care staff, and some content is not relevant to frontline staff in SME care providers e.g. the module on Freedom of Information.

3.1.2 The National Cyber Security Centre 'Staying Safe Online: Top Tips for Staff'

The National Cyber Security Centre (NCSC) has produced an e-learning training package: 'Staying Safe Online: Top Tips for Staff'. The training introduces why cyber security is important and how attacks happen, and then covers four areas:

- defending yourself against phishing
- using strong passwords

- securing your devices
- reporting incidents ('if in doubt, call it out')

The training is primarily aimed at SMEs, charities and the voluntary sector, but can be applied to any organisation, regardless of size or sector. It is designed for a non-technical audience and is suitable for all who use computers and phones for work purposes. Whilst not sector-specific, it has good generic advice on how to stay safe online and has a quiz at the end. It does not cover aspects of data security and protection that are not related to cyber security.

The e-learning package can be accessed directly by staff at https://www.ncsc.gov.uk/training/top-tips-for-staff-scorm-v2/scormcontent/index.html: no login is required. Care providers can also download a zip file, which contains the package as a SCORM-compliant file (or API version) so that they can host the course on their own learning management system (LMS) if they have one. Once imported into an LMS system, organisations can tweak the package to suit their needs (such as setting a quiz pass rate) as the content is covered by the Open Government Licence.

3.1.3 Digital Social Care training videos

Digital Social Care hosts 2 videos – available https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/train-staff-to-be-cyber-aware/ - that can be used for staff training:

Data protection care services training, which is seven minutes long, is aimed at frontline staff and can be used for staff training. The video covers what is personal data (and special category data) and what data is held in a care service, the importance of data security, and why it’s important to frontline staff. It also covers the six key principles of the General Data Protection Regulations (GDPR) and gives examples of how they could apply to care services.

Data and cyber security care services training, which is 11 minutes long, is aimed at frontline staff and can be used for staff training. The video provides a basic introduction to data and cyber security breaches and the steps you can take to avoid them, including how to use passwords to secure devices, logging in and out of systems and several top tips on spotting phishing and how to use email safely.

There is also a slightly longer video (16 minutes) called **Keeping your care service cyber secure** that is an introductory learning resource for managers / Data Security and Protection Leads. It defines cyber security then sets out 10 steps to keep digital devices cyber secure and where possible it gives practical advice about how to implement the steps. The video contains information on passwords and keeping devices safe, protecting mobile devices, backing up data and managing security relationships with suppliers as well as encouraging staff to report data breaches.

3.1.4 Skills for Care Learning resource: Cyber security

Skills for Care (SfC) has adapted the videos developed by Digital Social Care, described above, so that they can be used in team meetings or group learning sessions with a facilitator to encourage discussion and commitment to team and individual actions – available https://www.skillsforcare.org.uk/Support-for-leaders-and-managers/Managing-a-service/Digital-technology-and-social-care/Learning-resource-Cyber-security.aspx. On the SfC website the videos are called:

- Data and cyber security: introductory learning resource for frontline workers
- Six golden rules – GDPR learning resource for frontline staff
- Data and cyber security: introductory learning resource for managers

Each video is split into topic areas and there are on-screen questions at the end of each topic area. Most of the on-screen questions are open questions without a correct / incorrect response such as what steps can you take to reduce the risk of a data breach? There is Guidance for Managers and Facilitators to help facilitate the session and includes a summary of the animations and links to further guidance and resources to support staff training.

3.1.5 BT Skills for Tomorrow

BT offers free online courses and webinars about using digital devices and cyber security. They are not sector-specific, but the courses give clear, structured lessons from how to create strong passwords through to securing employee devices and networks. Technical aspects are presented in accessible language and, whilst these aspects are not covered in depth, there are good prompts as to what you need to think about. Each course has tests to check knowledge. Courses are split into Home Life and Work Life and there are webinars covering both.

Home Life has a section on basics for absolute beginners e.g. ‘video calling’ and ‘using the internet’ - that might be useful for some staff in adult social care. There is also a section on online safety that includes 10 minute training Staying safe online which will help people be more phishing and scammer aware and Keeping your device safe which explains how to protect your device and information on it from threats like viruses, and use of screen locks. Between them, these courses adequately cover the cyber security elements of threats to data security and knowing how to avoid them.

The Work Life stream has courses under the section ‘Business security’. Cyber security for business - the basics focuses on the types of cyber crime, how to protect a business, and what to do if your business is attacked. Improve your online business security is slightly more advanced and covers securing networks, systems and software, and employee devices. Neither of the business security courses are suitable for annual staff training but might help small care business owners or managers to learn the basics of online security and how it applies to their business.

3.1.6 Barclays Digital Wings

Barclays Digital Wings offers free online courses and webinars that aim to boost digital skills and confidence. They are not sector-specific, but the courses give clear, structured lessons and have tests to check knowledge. The courses cover a variety of topics including the comprehensive Keep safe online, which covers passwords, fraud and scams, protecting devices and protecting data. This course adequately covers the cyber security elements of threats to data security and knowing how to avoid them.

3.1.7 Gap analysis of free resources for annual training of staff against the learning outcomes of the NHS DSA training

Resource	1	2	3	4	5	6	7	8	9	Test	Comments
NHS - Data Security Awareness Level 1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Not suitable for frontline social care staff in SME care providers and only available online
NCSC - Top Tips for Staff	No	No	No	Partly	Partly	No	No	No	No	Yes	Does not cover physical security elements of threats to data security. Not specific to social care
Digital Social Care/ Skills for Care - Data protection care services training / Six golden rules	Yes	Yes	No	No	No	Yes	No	No	No	No	Whilst the SfC version has some discussion points that could be used at a team meeting or in a learning session, it does not have a mandatory assessment with a pass mark of 80%.
Digital Social Care/ Skills for Care - Data and cyber security care services training / introductory learning resource for frontline workers	Partly	No	Partly	Yes	Yes	No	No	No	No	No	Whilst the SfC version has some discussion points that could be used at a team meeting or in a learning session, it does not have a mandatory assessment with a pass mark of 80%.
BT Skills for Tomorrow – Staying safe online and Keeping your device safe	No	No	No	Partly	No	No	No	No	No	Yes	Does not cover physical security elements of threats to data security. Not specific to social care
Barclays Digital Wings – Keep safe online	No	No	No	Partly	No	No	No	No	No	Yes	Does not cover physical security elements of threats to data security. Not specific to social care

3.2 Resources for training specialist roles

3.2.1 Data Security and Protection Lead

The Data Security and Protection Lead (DSPL) is a relatively new role for social care and, potentially, it exists in conjunction with several other roles that are not currently mandatory for SME care providers. Skill for Care has developed a job description for this role.

In lieu of any minimum standards for training for the role, in their guide to Data Security and Protection: roles and responsibilities, Digital Social Care recommended that the Data Security and Protection Lead completes the national NHS eLearning course Data Security Awareness or equivalent. More recently, the Institute of Public Care and Skills for Care developed a webinar for Data Security and Protection Leads to introduce this role and outlines what the role covers. A recording of that webinar is available at https://www.digitalsocialcare.co.uk/digital-skills-and-training/data-security-and-protection-lead-training/. The webinar does not offer detailed or in-depth training but outlines 8 key areas that the Lead should take responsibility for and gives links to further information about those areas (including to the Digital Social Care video Keeping your care service cyber secure).

3.2.2 Caldicott Guardian

Guidance about the appointment of Caldicott Guardians, their role and responsibilities was published by the National Data Guardian for Health and Social Care (NDG) in 2021. Previously, only NHS organisations and local authorities were required to have a Caldicott Guardian. This guidance changes that, by widening the requirement to include organisations providing publicly funded adult social care or adult carer support. Organisations are encouraged to be **compliant with the NDG guidance by 30 June 2023**.

We undertook a programme of research to explore how the Caldicott Guardian role is represented in the sector currently and how these could be embedded into care organisations to meet the new NDG guidance. **Further information about our findings on the Caldicott Guardian role are appended**.

The UK Caldicot Guardian Council (UKCGC) is the key resource and ‘go to’ place for new and experienced Caldicott Guardians alike. The UKCGC has developed a range of resources for Caldicott Guardians, including the **Caldicott Guardian Manual** (https://www.ukcgc.uk/manual/contents). The manual is intended to be a starting point for newly appointed Caldicott Guardians, a refresher for the more experienced, and a pointer to possibilities for professional development and support

As well as the manual and other resources, specialist training for Caldicott Guardians is available. The UKCGC lists the following providers that offer specialist training and events for Caldicott Guardians:

- Healthcare Conferences UK provide conferences, masterclasses and courses. There is a one-day CPD certified training course - currently virtual, used to be face to face – that costs £295 plus VAT. This course was undertaken by all our interviewees who had undertaken formal training for the Caldicott role. Feedback from interviews was that the course, whilst very good, was very health focussed.

- Stay Compliant Training provides a one-day CPD accredited course for Caldicott Guardians that costs £275 for an online course and £299 for face to face delivery.
- Leadership Through Data provides a one-day online CPD accredited course for Caldicott Guardians that costs £375 plus VAT.

The UKCGC, with Health Education England, has recently developed an **eLearning programme** 'The Role of the Caldicott Guardian' that is available free of charge on the eLearning for healthcare portal. The learning is aimed at all staff in health and social care and explains the part that Caldicott Guardians play in keeping data safe and ensuring that wise decisions are made about its use. The Council is planning to develop two further eLearning modules:

- A session for new or existing Caldicott Guardians
- A session for senior staff who may need to appoint or support a Caldicott Guardian

The case studies and, to a lesser extent, the terminology used in the eLearning is very health focussed. In addition, it assumes that Caldicott Guardians will work in larger organisations that are able to have a separation of roles and responsibilities. For example, it states *"The Caldicott Guardian should work as part of a broader IG function"*. The resources do not explore how small organisations - who may not be able to have separate people holding key roles such as the SIRO, DSPL and Caldicott Guardian - manage the potential conflicts of interests that this might bring and ensure that the Caldicott Guardian principles are understood and implemented even if no Caldicott Guardian is appointed.

3.3 Resources for induction

The Care Certificate was developed jointly by Skills for Care, Health Education England and Skills for Health. It is an agreed set of standards that define the knowledge, skills and behaviours expected of certain roles in social care. Designed with the non-regulated workforce in mind, the Care Certificate aims to give everyone the same introductory skills, knowledge and behaviours and offers a structured practical induction programme to make sure new care workers are effectively prepared for their role. As such, care providers rely on it to meet evidence item 2.1.1 about the induction process.

The Care Certificate is made up of the 15 minimum standards that should be covered if you are 'new to care'. Standard 14 Handling Information has the learning outcomes:

14.1a Describe the agreed ways of working and legislation regarding the recording, storing and sharing of information
14.1b Explain why it is important to have secure systems for recording, storing and sharing information
14.1c Demonstrate how to keep records that are up to date, complete, accurate and legible
14.1d Explain how, and to whom, to report if they become aware that agreed ways of working have not been followed

The table below reviews standard 14 workbook against the minimum standard of induction to comply with the DSPT, which highlights that the Care Certificate does not fully meet the requirement to help staff understand their obligations under the National Data Guardian's (NDG) data security standards in their organisation.

	Learning outcome	Analysis	Comments
A)	The importance of data security in the care system	Met	Covers records well but little focus on digital data security
B)	The NDG data security standards, particularly the three standards relating to personal responsibility (standards 1, 2 and 3)	Not Met	This is not covered.
C)	The applicable laws (GDPR, FOI etc) knowing when and how to share and not to share	Met	A light touch approach with a link for learners to look up more information. More could be included within the Standard 14 training as the link to the ICO is in-depth, too much detail and won't all be relevant to social care staff
D)	Understanding threats to data security: i. what social engineering is ii. safe use of social media and email iii. the dangers of malicious software iv. how to protect information v. physical security	Partly Met	A light touch on not sharing passwords. Highlights the increased use of mobile technology and the use of social media. More in-depth coverage of cyber security and what safe practice looks like is needed
E)	Knowing how to spot and report data security breaches and incidents	Partly Met	Focusses on 'confidentiality' and reporting. No explanation around 'integrity' and 'availability' of data and how these three elements work together How to identify data breaches not covered.

4 A skills assessment for care providers

We carried out engagement and consultation to explore if a skills assessment would support care providers to ensure their staff are DSPT compliant rather than repeated annual training.

There was a consensus that a national resource of short, snappy training resources, designed specifically for the social care sector, which can be used flexibly online and offline, was needed to enable more SME care providers to meet the DSPT requirement set out in 3.2.1. It was felt that care providers don't know where to turn to get the right training or what it should cover.

We developed and tested two learning tools – an assessment for frontline staff and a manager's discussion tool - that can be used flexibly to help care providers to meet the DSPT training requirements, including the need for staff to undertake an assessment and gain an 80% pass mark. The assessment tool is based on four proposed learning outcomes suitable for frontline social care staff.

The proposed learning outcomes and assessment tool were unilaterally well received, with feedback reflecting that they were pitched at the right level, language and content for frontline care staff. Comments included:

"I am delighted to finally see a resource that really has been developed by people who understand the sector!"

"I like this and see it used in team meetings and supervisions, used in bite sized segments".

"I think that the quiz questions look absolutely perfect and will clearly demonstrate whether the required learning has taken place or not."

"I really like the structure that has been laid out for the providers, indicating exactly which topics should be covered and indicating the depth to which they need to go. My strong feeling is that the best way to deliver the training (to actually get engagement) is to offer an online training programme which includes the quiz and is certified and possibly provides continuous professional development credit."

Most of those consulted felt that they would use the managers' discussion tool in team discussions, where they would ideally play a short video and conduct a discussion using the prompts within the tool, but it could be used flexibly in a number of ways. They highlighted the need for discussions to include scenarios which staff would recognise to make the training relevant to them and then set or work through the multiple choice quiz either individually, in pairs or in small groups. Managers also saw themselves using the multiple choice quiz as a tool to assess learning needs.

Care providers felt that this resource would best be hosted by Skills for Care or a similarly recognised and respected sector-based organisation in an easily downloadable format.

However, as well received as the assessment tool was, consultees made the point that it needed to be complemented by a national learning resource appropriate for frontline staff in the social care sector. There was also feedback that a higher level of training (specific to social care) needs to be developed for more senior staff with responsibility for data security and protection. Both need to be easy to access and available to use offline as well as online and in a format which those organisations with online learning management systems can import into their system.

5 Conclusions and recommendations

There is no easy to access, free and sector-appropriate national training available to social care providers:

- Whilst the NHS Data Security Awareness Level 1 training meets the National Data Guardian's requirements for evidence item 3.2.1, it is difficult to access for non NHS staff and not suitable for frontline staff in SME care provider organisations. In addition, it is only available as an eLearning module and some social care staff do not have access to the internet for work purposes.
- Some excellent cyber security training modules exist (from NCSC, BT and Barclays) that include a skills assessment. However, they do not cover the non-digital elements of threats to data security nor the wider data protection / information governance aspects of the requirements.
- Between them, the two Digital Social Care / Skills for Care training videos cover many of the requirements for evidence item 3.2.1, but not all, and they do not have a linked skills assessment. Equally important, they are not badged as such and so care providers would not know that these videos could contribute to meeting the requirements for training 95% of staff.
- The Care Certificate does not fully meet the National Data Guardian's requirements for evidence items 3.2.1 or 2.1.1

We developed and tested an assessment tool that can be used flexibly to help care providers to meet the DSPT training requirements, including the need for staff to undertake an assessment and gain an 80% pass mark. The proposed learning outcomes and draft assessment tool were unilaterally well received, with feedback reflecting that they were pitched at the right level, language and content for frontline care staff. Consultees were extremely positive about the assessment tool with care organisations keen to adopt it as soon as it becomes available and offering to pilot it, or part of it, with their care staff. However, as well received as the assessment tool was, it needs to be complemented by free, national training appropriate for frontline staff in the social care sector.

There is also a need to develop a higher level of training, which is specific to social care, for more senior staff with responsibility for data and cyber security. The Data Security and Protection Lead (DSPL) is a relatively new role for social care and, whilst there is an awareness raising webinar, no detailed training for care providers is available. The Caldicott Guardian eLearning modules developed by the UKCGC are health focussed and assume that Caldicott Guardians work in larger organisations that have a separation of roles and responsibilities. The interrelation between specialist roles in small organisations - who may not be able to have separate people holding key roles such as the SIRO, DSPL and Caldicott Guardian – should be explored further in the training resources. We think that this is a key gap for training and support that is appropriate for SME care providers as well as more guidance on the circumstances that might lead an organisation not to appoint a Caldicott Guardian.

All national training needs to be easy to access and available to use offline as well as online and in a format which organisations with online learning management systems can import into their own systems.

Recommendation
Key sector stakeholders should be involved in the development of a national learning resource that meets the needs of the range of small social care providers completing the DSPT and is accepted as meeting the minimum requirements for frontline staff training (evidence item 3.2.1). The learning outcomes for frontline social care staff should be:

1. Understand the importance of data security and protection in the care system and your personal responsibility to handle data safely
2. Be able to apply relevant data security and protection legislation and principles
3. Be aware of physical and digital threats to data security and know how to avoid them, including:
   i. being alert to social engineering
   ii. safe use of digital devices
   iii. safe keeping of physical records
4. Be able to identify data breaches and incidents and know what to do if one happens

The training resource should include the assessment tool we developed, additional videos to support that tool, and a training course, which is available in non-digital as well as digital formats and is easily accessible (without login required) from a well-known sector support organisation(s) such as Skills for Care or Digital Social Care. The training course should include scenarios which make it relevant to frontline care and ancillary staff.

Recommendation
Amend DSPT evidence item 3.2.1 tooltip to refer people to the national learning resource described above. In the meantime, publish the assessment tool we developed and provide clarity on the learning outcomes and minimum requirements for frontline staff training on a dedicated webpage on Digital Social Care (currently the tooltip refers people to Cyber Security Training for Staff).

Recommendation
The Better Security, Better Care programme should work with the UKCGC and other key sector stakeholders to develop free national learning resources that are appropriate for specialist roles in SME social care providers. This should include:

- Revising the Digital Social Care resource Data Security and Protection Responsibilities and Skill for Care job description for this role to take account of the changes to the Caldicott Guardian guidance.
- Building on the webinar produced by Skills for Care and the Institute of Public Care to develop a training course for Data Security and Protection Leads.
- Developing new version(s) of the Caldicott Guardian eLearning modules, that the UKCGC has developed with Health Education England, to meet the needs of SME care providers.

Importantly, these training materials will need to unpick how social care organisations of different sizes could meet the requirements in the NDG guidance, including that the Caldicott Guardian principles are understood and implemented even if no Caldicott Guardian is appointed. The training materials should be available in non-digital as well as digital formats and easily accessible (without login required) from a well-known sector support organisation such as Skills for Care or Digital Social Care.

Recommendation
As well as developing sector specific annual training for frontline staff and specialist roles, we recommend that the Care Certificate is also reviewed and revised. Care providers rely on it for induction of new staff, but currently it does not fully meet the National Data Guardian's requirements for evidence item 2.1.1.

Recommendation
Small and micro care providers may want to appoint an external Caldicott Guardian. We think that care provider membership organisations might be feasible hosts for such an arrangement in some parts of the country, but this needs to be explored further, and funding a pilot of this in 2022 should be considered. There is scoping work to be done to understand the mechanism, scale and cost of hosting a Caldicott Guardian service.

Recommendation
The change to the Caldicott Guardian role due in 2023 needs an education campaign relevant to all stakeholders in the sector. A communication campaign, through channels proven to be effective, that acknowledges the state of the social care sector, explains the importance and purpose of the Caldicott Guardian role, reassures care providers of its feasibility, and promotes sector specific resources is urged.

6 Appendix – research on Caldicott Guardians

Guidance about the appointment of Caldicott Guardians, their role and responsibilities was published by the National Data Guardian for Health and Social Care (NDG) in 2021. Previously, only NHS organisations and local authorities were required to have a Caldicott Guardian. This guidance changes that, by widening the requirement to include organisations providing publicly funded adult social care or adult carer support. Now, these organisations are being asked to put in place a Caldicott Guardian, whether by appointing a member of their own staff or making other arrangements. The guidance states that:

- Caldicott Guardians will operate differently depending on type or size of organisation (2.8 of NDG guidance).
- An individual may undertake the Caldicott Guardian role in addition to another role or duty within their organisation (3.2 of NDG guidance).
- Caldicott Guardians must be afforded the freedom to raise concerns at senior management or board level (6.3 of NDG guidance).
- If it is not proportionate or feasible for an organisation to appoint a member of its own staff to the Caldicott Guardian role, it should arrange for the function to be provided in another way (3.4 of NDG guidance).
- If an organisation chooses not to appoint a Caldicott Guardian, it should document this decision and the reasons for it (3.7 of NDG guidance).

Organisations are encouraged to be **compliant with the NDG guidance by 30 June 2023**. This includes registering the details of their Caldicott Guardian(s) on the Caldicott Guardian Register and providing details about its Caldicott Guardian(s) as part of their DSPT submission. There is likely to be widespread ignorance of the new guidance for appointing Caldicott Guardians among both care providers and the sector at large.

Caldicott Guardians are senior people within an organisation who make sure that the personal information about those who use the organisation's services is used legally, ethically and appropriately, and that confidentiality is maintained. They ensure that the eight Caldicott Principles are upheld by their organisation.

We undertook a programme of research to explore how the DPO and Caldicott Guardian roles are represented in the sector currently and how these could be embedded into care organisations to meet the new NDG guidance. As well as desk research, we interviewed and met with seven Caldicott Guardians and DPOs working in the sector, the UK Caldicott Guardian Council (UKCGC) and Caldicott Guardian training providers, plus a range of adult social care stakeholders and organisations from health and information governance.

There are four possible options for care providers to meet the new guidance:

1. Appoint an internal Caldicott Guardian
2. Share a Caldicott Guardian with other providers
3. Appoint an external Caldicott Guardian
4. Not appoint a Caldicott Guardian, and document the reasons

The advantages of an internal Caldicott Guardian is that the individual knows the organisation, is on site to detect Caldicott Guardian issues when they occur, can inculcate a good attitude to data security and protection within the organisation, can ensure that the right policies and procedures are in place, and can engender the trust of colleagues to raise issues.

Appointing an internal Caldicott Guardian requires the organisation to have someone suitable with sufficient capacity and seniority to take on the role. The Caldicott Guardian role involves training, on-going development and time to execute it. Paid for training already exists; free e-learning is in development; high quality free advice and support in the form of the UKCGC already exists - but the current resources are not suitable for the social care sector. In theory, all sizes of care provider could appoint their own Caldicott Guardian, and large and medium sized providers may well choose to do so. However, in reality, the micro and small care provider is highly unlikely to have the resources – human or financial - to appoint an internal Caldicott Guardian. If they do, there is a danger of it being a Caldicott Guardian in name only.

Care providers sharing a Caldicott Guardian with other local care providers presents several difficulties. A larger care provider with a Caldicott Guardian in post providing the service to other smaller care providers would be likely to prioritise their own organisation. Small care providers sharing a Caldicott Guardian on a more equal footing presents the practical problem of finding an organisation willing to take the lead organising a complex arrangement involving confidential data, costs and membership rules.

Appointing an external Caldicott Guardian is an option for all sizes of care provider. The care sector is familiar with appointing external DPOs, IT and HR services. We identified possible hosts for such an arrangement as: commissioners, commercial consultancies, and care provider membership organisations.

A, probably, insurmountable drawback to commissioners hosting a Caldicott Guardian service is the procurement relationship between commissioners and their suppliers.

The fees charged by data protection or information governance consultancy companies are too high for many small care providers. An individual data protection consultant or very small consultancy’s are likely to be more reasonable but may still be too much.

Care provider membership organisations, local and national, appear to be a natural place for care providers to find an external Caldicott Guardian; they provide other services to members, they understand the sector, have a close relationship with their members, and are trusted by them. There is scoping work to be done to understand the mechanism and scale of membership organisations hosting a Caldicott Guardian service. A helpline combined with an annual audit could be a model and a pilot is urged to scope out the mechanism and resource required. The scoping would need to include cost structure, for example whether it is absorbed into the membership package or is an additional paid for service, scale and minimum service offer acceptable.

The NDG guidance offers the option of not appointing a Caldicott Guardian, as long as the reasons for this decision are documented. However, there is an expectation that the ‘Caldicott Function’ is adhered to, that is, for the organisation to evidence that the Caldicott Guardian principles are understood and implemented.