Data Security Standard 3
Training

The bigger picture and how the standard fits in

July 2017
Contents

Overview 3

Learning Needs Analysis 4

What are the objectives of an LNA? 4
Benefits and outcomes 4
Knowing your staff 4
LNA approval 6
National training for all staff 6
National training a minimum not a maximum 6
Specialist staff training 7
Leaders and board members 7
Caldicott Guardians 7

Appendix 1 - Table of Data Security Level 3 Assertions 9
Appendix 2 - Useful resources 10
Appendix 3 – The National Data Guardian Reports 11
Overview

The NDG’s review data standard 3 states that

“All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.”

Our staff can be the greatest asset in spotting data security and protection issues and incidents. Unfortunately, they can also be exploited and inadvertently bypass controls that are in place. Our collective goal is to empower staff with sufficient, up-to-date knowledge, allowing them insight and resilience.
Learning Needs Analysis

Knowing your staff

The acceptance of the National Data Guardian’s 10 data standards by Her Majesty’s Government has changed our approach to information sharing and security. In order to fulfil Data Security Standard 3, you need to assess your organisation’s learning needs. This can be accomplished by a learning (or training) 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. At their heart, LNAs are about knowing your staff and making sure that their training needs are met. This helps them as well as improving your organisation’s data security.

What are the objectives of an LNA?

An LNA process is the way in which you can establish the training requirements of your staff. It will also allow you to plan associated training activities and develop a training plan. This is explained in more detail below.

Benefits and outcomes

There are many benefits to carrying out LNA. It:

- helps to identify possible risks that may affect the training;
- identifies resource requirements and restrictions;
- establishes pre-requisites for the training early in the process.

“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

MANDATORY: There has been an assessment of data security and protection training needs across the organisation. A training needs analysis has been completed

Data Security Standard 3.1
LNA methods

As a small social care organisation, there is no need to complete a highly formal LNA with data analysis, unless you feel that this would benefit your organisation. It is understood that this may well be the first time an LNA has been used and that you may not have any existing information sharing training in your existing training matrix.

The following method should be followed:

1. Assess what training is already in place in your organisation for all staff. This will act as your baseline. You may have nothing in place at the moment, which gives you a clean slate to implement training.

2. Identify the scope of the LNA: who should be included and excluded, e.g. maternity / paternity, long-term sick and agency staff.

3. Some members of your staff will need a higher level of knowledge around information security and sharing than the rest. For example, the Data Security and Protection Lead or senior staff who often handle and have to make decisions about personal information.

4. Making a note of each of these steps and ensuring that each decision is signed off by the necessary person in your organisation will be evidence for your LNA.

It is worth considering if you would need to provide more training for members of staff who use computers or mobile devices in the course of their work, as compared to any staff whose work is completely paper based.
LNA approval

Before implementing any new training, you must have sign off from the person responsible for information security in your organisation. This may be the SIRO (Senior Information Risk Owner).

**National training for all staff**

All staff must complete appropriate data security training. National training has been developed with the assistance of various health and social care organisations. This training is freely available to everyone working in social care.

The Data Awareness Training Level One is aimed at all staff and is followed by a test which evidences that the staff member understands the material. The training includes a number of realistic and relevant case studies. The link for the training can be found in Appendix 2 below.

The national training provided is not the only option and local training which covers the same material is also acceptable.

In order to register for e-learning, social care organisations will need to know their ODS code. This is a unique identifier which is assigned for you by the NHS. If you do not know your code you can contact exeter.helpdesk@nhs.net and they will help you or you can look it up at the ODS portal: [https://odsportal.hscic.gov.uk/](https://odsportal.hscic.gov.uk/) if you have access to N3 or HSCN.

**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.

**Staff pass the data security and protection mandatory test**

---

Data Security Standard 3.1.3

Data Security Standard 3.3
Specialist staff training

In addition to the training for all staff, those with specialist roles should receive the benefit of specialist training in data security and protection. The type of roles this is aimed at may include:

- Information Governance Lead(s)/ Data Security Leads
- Information / Data / Cyber Security staff (if a separate role to IG Lead)
- senior management
- Quality Assurance staff (if any).

This list is not exhaustive.

Leaders and board members

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

Data Security Standard 3.4

The National Data Guardian’s review (appendix 3) identified the tremendous benefit to organisations who have actively engaged leaders. At least one senior person within the organisation should be able to champion data security at the highest level of your organisation.

Caldicott Guardians

Leaders and board members receive suitable data protection and security training

Data Security Standard 3.5

It is the Caldicott Guardian’s responsibility to ensure individual rights are respected when it comes to information sharing and data security; not every care home will have a Caldicott Guardian. If you feel that your organisation would benefit from having a Caldicott Guardian, then they should be supported with specialist training. There is more information available about Caldicott Guardians here:

https://www.gov.uk/government/groups/uk-caldicott-guardian-council
Aside from the data security and protection training that all staff undertake. Caldicott Guardians training is currently in the form of a standalone workbook which resides at the following location:

https://www.igt.hscic.gov.uk/WhatsNewDocuments/The%20Role%20of%20the%20Caldicott%20Guardian-%20Workbook-28-03-2017-Published.docx.
### Appendix 1 - Table of Data Security Level 3 Assertions

<table>
<thead>
<tr>
<th>Assertion</th>
<th>Baseline Assertion</th>
<th>Sub Assertion</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3.1 There has been an assessment of data security and protection training needs across the organisation</strong></td>
<td>Yes</td>
<td>3.1.1</td>
<td>A data security and protection training needs analysis has been completed.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>3.1.2</td>
<td>Date of last data security and protection training needs analysis</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>3.1.3</td>
<td>Training Needs analysis has been approved by the person with overall responsibility for data security.</td>
</tr>
<tr>
<td><strong>3.2 Staff receive suitable data security and protection training</strong></td>
<td>No</td>
<td>3.2.1</td>
<td>Staff awareness – Training (Q12) … The data security training offered by my organisation supports me in understanding how to use data lawfully and securely</td>
</tr>
<tr>
<td><strong>3.3 Staff pass the data security and protection mandatory test</strong></td>
<td>Yes</td>
<td>3.3.1</td>
<td>Percentage of Staff Successfully Completing the Level 1 Data Security Awareness training.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>3.3.2</td>
<td>Average mark of first attempt of Level 1 Training</td>
</tr>
<tr>
<td><strong>3.4 Staff with specialist roles receive data security and protection training suitable to their role</strong></td>
<td>Yes</td>
<td>3.4.1</td>
<td>Number of staff assessed as needing role specialist training</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>3.4.2</td>
<td>Number of staff completing advanced Data Security Training.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>3.4.3</td>
<td>Details of any specialist data security and protection training undertaken.</td>
</tr>
<tr>
<td><strong>3.5 Leaders and board members receive suitable data protection and security training</strong></td>
<td>Yes</td>
<td>3.5.1</td>
<td>SIRO and Caldicott Guardian have received appropriate training.</td>
</tr>
</tbody>
</table>
Appendix 2 - Useful resources

Care Provider Alliance

They have provided more information about the e-Learning for Healthcare training and how to access this:


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

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://www.e-lfh.org.uk/

NHS Digital ODS (Organisation Data Service)

Responsible for publishing codes that identify organisations and individuals across health and social care.

https://odsportal.hscic.gov.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