Data Security Standard 2
Staff responsibilities

The bigger picture and how the standard fits in 2018
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Systems holding personal confidential information</td>
<td>4</td>
</tr>
<tr>
<td>Definitions and scope</td>
<td>4</td>
</tr>
<tr>
<td>List of systems holding PCI</td>
<td>5</td>
</tr>
<tr>
<td>SIRO / senior management involvement</td>
<td>5</td>
</tr>
<tr>
<td>Data protection and security induction</td>
<td>6</td>
</tr>
<tr>
<td>Delivery of the induction</td>
<td>7</td>
</tr>
<tr>
<td>Staff scope</td>
<td>7</td>
</tr>
<tr>
<td>Review</td>
<td>7</td>
</tr>
<tr>
<td>Staff contracts</td>
<td>8</td>
</tr>
<tr>
<td>Appendix 1 -</td>
<td>9</td>
</tr>
<tr>
<td>Table of Data Security Level 2 Assertions</td>
<td>9</td>
</tr>
<tr>
<td>Appendix 2 -</td>
<td>11</td>
</tr>
<tr>
<td>Useful resources</td>
<td>11</td>
</tr>
<tr>
<td>Appendix 3 –</td>
<td>12</td>
</tr>
<tr>
<td>The National Data Guardian Reports</td>
<td>12</td>
</tr>
</tbody>
</table>
Overview

The National Data Guardian (NDG) review’s data standard 2 states that:

“All staff understand their responsibilities under the National Data Guardian’s Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.”

All staff understand what constitutes deliberate, negligent or complacent behaviour and the implications for their employment. They are made aware that their usage of IT systems is logged and attributable to them personally. Insecure behaviours are reported without fear of recrimination and procedures which prompt insecure workarounds are reported, with action taken.
Systems holding personal confidential information

Definitions and scope

Personal confidential information (PCI) is personal and usually sensitive confidential information that is held by your organisation and is subject to an obligation of confidentiality. The two types of people in focus are staff and patients / service users. Personal Confidential information is likely to include (but is not limited to) information about a person’s:

- physical or mental health
- social or family circumstance
- financial standing and financial details
- education, training and employment experience
- religious beliefs
- racial or ethnic origin
- sexuality
- criminal convictions
- genomic data
- biometric data (e.g. fingerprints)
- IP address.

Confidential personal information would be held in systems such as:

- care planning systems
- staff rostering systems
- payroll
- electronic medication administration systems.

There is a clear understanding of what Personal Confidential Information is held.

Data Security Standard 2.1
List of systems holding PCI

A list of systems holding PCI should be maintained.

There is not a prescribed method, however, this can be recorded in an information asset register (IAR). There is a template IAR linked in Appendix 2 below.

An IAR should include a record of digital and hard copy records, who is responsible for ensuring the safety of the record, and what safety measures are in place. For example, you might look at your archived care records and decide that it makes most sense for your registered manager to be responsible for these records and that the safety procedures in place are that they are locked in a filing cabinet in a room which is locked when not in use.

You should review this list periodically and amend if there are changes.

MANDATORY: When was the last review of the list of all systems/information assets holding or sharing personal information?

SIRO / senior management involvement

Someone in senior management in your organisation should have responsibility for managing information risks – this might be your data security and protection lead or maybe someone with a different job role.

Within the NHS the person with this responsibility is often called a “Senior Information Risk Owner (SIRO)”, you can choose whether you want to use this title or not as long as someone is taking on this job role.

The important thing is that your information asset register, or list of systems, should be signed off by someone suitably high up in your organisation.
Data protection and security induction

When staff start with a new organisation, it is during their induction period when they can be at their most vulnerable. They may not understand the organisation’s systems, policies and procedures, its cultures or norms.

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:

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

“**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.**”

*BMA*

**Your Data: Better Security, Better Choice, Better Care**

**Government Response**

It is important that the messages are local and specific to your organisation and that they include local procedures and policies and if possible local incidents.

**MANDATORY:** There is a data protection and security induction in place for all new entrants to the organisation.

Data Security Standard 2.3.1
Delivery of the induction

There are no stringent guidelines on how the course is delivered, however it is important that it is effective and resonates with your audience. Some of the delivery methods you can consider are:

- a discreet separate event
- part of a wider employee induction
- face to face
- digital delivery (such as e-learning).

Staff scope

It is important that a record is kept of all staff at your organisation who have received appropriate training and when this is due for renewal. This also includes staff who work at, but not directly for, your organisation (such as agency staff). The organisation either needs to verify that the training received by agency staff is satisfactory or ensure that those staff attend the organisation’s induction.

Review

It is good practice to encourage staff to provide feedback on the induction itself in order improve it, but to also regularly review the content to ensure it is relevant and up to date.
Staff contracts

Appropriate clauses in staff contracts should reference data security (confidentiality, integrity and availability). It is recognised that most contracts commonly focus on confidentiality clauses.

If you are managing third party personnel, you are likely be managing them through a contract as discussed in Data Security Standard 10 ‘Accountable suppliers’ i.e. your contract refers to contractor data security and protection training.

MANDATORY: All employment contracts contain data security requirements.

Data Security Standard 2.3.2
## Appendix 1 -
### Table of Data Security Level 2 Assertions

<table>
<thead>
<tr>
<th>Assertion</th>
<th>Mandatory</th>
<th>Sub Assertion</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2.1 There is a clear understanding of what Personal Confidential Information is held.</strong></td>
<td>Yes</td>
<td>2.1.1</td>
<td>When was the last review of the list of all systems/information assets holding or sharing personal information?</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>2.1.2</td>
<td>The list of all systems/information assets holding or sharing personal confidential information has been approved as being accurate by the person with overall responsibility for data security.</td>
</tr>
<tr>
<td><strong>2.2 Personal Confidential Information is processed / shared legally and securely.</strong></td>
<td>No</td>
<td>2.2.1</td>
<td>Staff awareness - Shared securely (Q5) …. I know how to use and transmit data securely.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>2.2.2</td>
<td>Staff awareness - Used legally and securely (Q6) …. I am happy data is used legally and securely in my organisation.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>2.2.3</td>
<td>Staff awareness - Processes (Q7) …. The tools and processes used by my organisation make it easy to use and transmit data securely.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>2.2.4</td>
<td>Staff awareness - Raising concern (Q8) …. I can raise concerns about unsecure or unlawful uses of data, and I know that these will be acted on without personal recrimination.</td>
</tr>
<tr>
<td><strong>2.3 Staff are supported in understanding their obligations under the National Data Guardian’s Data Security Standards.</strong></td>
<td>Yes</td>
<td>2.3.1</td>
<td>There is a data protection and security induction in place for all new entrants to the organisation.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>2.3.2</td>
<td>All employment contracts contain data security requirements.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>2.3.3</td>
<td>Staff awareness - Laws and principles (Q9) …. I understand the important laws and principles on data sharing, and when I should and should not share data.</td>
</tr>
<tr>
<td>No</td>
<td>2.3.4</td>
<td>Staff awareness - Data sharing questions (Q10) …. If I have a question about sharing data lawfully and securely I know where to seek help.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>2.3.5</td>
<td>Staff awareness - Personal responsibility (Q11)…. I take personal responsibility for handling data securely.</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 2 - Useful resources

Care Provider Alliance

The Care Provider Alliance has template documents for Information Asset Registers and Staff Contracts:


Skills for Care

Skills for Care’s Care Certificate outlines standards for robust inductions for individuals who are new to care. Standard 14 covers information handling.


Data and cyber security: protecting information and data in health and care: NHS Digital data security homepage

Links to news and guidance for organisations to support health and care to keep patient information and computer systems safe.

https://digital.nhs.uk/cyber-security

Guidance: National Cyber Security Centre

Expert, trusted, and independent guidance for UK industry, government departments, the critical national infrastructure and private SMEs. All our guidance is advisory in nature and is underpinned by our unique insights into cyber threats.

https://www.ncsc.gov.uk/guidance
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.

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.