Data Security and Protection Toolkit

# Strengthening Assurance- Independent Assessment and Audit Framework

## IT Suppliers and independent sector Operators of Essential Service (OES)

2024/25 Version 7 DSPT (NDG)

Creating a culture of Improvement

Information and technology for better health and care

09/09/2024

# Document Control

## Revision history

| Revision Date | Summary of changes | Changes marked | Version Number |
|---|---|---|---|
| 04/10/2019 | Initial Draft for consultation | 00/00/2019 | 1.0 |
| 28/04/2020 | Updated for DSP Toolkit Changes to the Standard and Guidance for 2020-21 and updated navigation links | | 1.1 |
| 10/06/2020 | Updated to include new evidence item (4.5.2) and associated guidance | 10/06/2020 | 1.9 |
| 30/06/2020 | Updated to include new evidence items (9.5.1 and reference to professional judgement & Big Picture Guide) | 30/06/2020 | 1.13 |
| 20/11/2020 | Updated to reflect revised wording of evidence items | 22/11/2020 | 1.13 |
| 18/01/2021 | Updated to correct mandatory status of evidence items and remove items no longer relevant for Categories 3 and 4 | 18/01/2021 | 1.14 |
| 29/01/2021 | Updated to remove out of date reference concerning sample sizes | 29/01/2021 | 1.15 |
| 30/06/2021 | Updated in line with 2021-22 DSPT Standard | 29/07/2021 | 1.16 |
| 16/09/2021 | Updated to address feedback and correct links | 16/09/2021 | 1.17 |
| 24/11/2021 | Updated to correct 8.1.3 assessment evidence | 24/11/2021 | 1.18 |
| 06/12/2021 | Updated to correct assessment guidance for 1.1.3 for category 2 organisations | 06/12/2021 | 1.19 |
| 14/12/2021 | Updated to remove reference to ‘whitelisting’ and ‘blacklisting’ | 15/12/2021 | 1.20 |
| 07/02/2022 | Updated 1.3.6 to be non-mandatory for Cat 3 | 07/02/2022 | 1.21 |
| 26/09/2022 | Updated to Ver 5 (22/23) of the DSPT Standard | 26/09/2022 | 1.22 |
| 15/2/2023 | Clarified 1.3.8 to being biennial | 15/2/2023 | 1.24 |
| 13/9/2023 | Updated to reflect latest version and removed cat 3 & 4 | 13/9/2023 | 1.25 |
| 12/9/2024 | Updated to v7 amended scope to category 2 only | 12/9/2024 | 1.26 |

Document Control: The controlled copy of this document is maintained by NHS England's Cyber Operations. Updates will be managed in accordance with changes made to the Data Security and Protection (DSP) Toolkit. It is expected that this document will be updated at least annually. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

# DSP Toolkit Independent Assessment Framework - Introduction

The NHS England Data Security and Protection Toolkit (DSP Toolkit) Independent Assessment Framework is a resource, created by NHS England, for independent assessors and auditors of Health and Social Care organisations. It is designed to be used with reference to the 'NHS England DSP Toolkit Independent Assessment Guide' and the 'NHS England DSP Toolkit Independent Assessment - Summary'.

This resource is the framework that the internal auditor or assessor must use to assess the organisation's data security and data protection controls against the requirements of the DSP Toolkit. It should act as the basis of scoping the terms of reference for each DSP Toolkit audit or assessment, the approach that the auditor or independent assessor should take during their review, and the evidence that the assessor should request and review as part of their work.

Further detail on the framework, and how to navigate it, is provided in the following pages. For each of the evidence items within the DSP Toolkit, the DSP Toolkit Independent Assessment Framework outlines the control objective of the evidence item, provides a step by step guide as to how to audit or assess the organisation's control environment against the objective, and an indication as to the on-site tests that could be performed and documents that the assessor should request and review as part of their work. It also includes details on whether or not the evidence item is mandatory for each category of health and social care organisation.

**The framework is designed to be used by individuals with experience in reviewing data security and data protection control environments. The assessment approach is not intended to be exhaustive or overly prescriptive, though it does aim to promote consistency of approach. Auditors and assessors are expected to use their professional judgement and expertise in further investigating and analysing the specific control environment, and associated risk, of each health and social care organisation.**

# DSP Toolkit Independent Assessment Framework - Introduction

It is essential that the review considers **whether the Health and Social Care Organisation meets the requirement of each evidence item**, and also considers the broader **maturity of the organisation's data security and protection control environment**. It should be noted that some of the framework approach steps go beyond what is asked in the DSP Toolkit. This is intentional and is designed to help inform the assessor's view of the organisation's broader data security and protection control environment. The intention is to inform and drive measurable improvement of data security across the NHS and not just simply assess compliance with the DSP Toolkit.

It is important, particularly for technical controls, that the independent assessor does not rely solely on the existence of policies and/or procedures, but reviews the operation of the technical control, preferably whilst on-site. For example, in evidence item 8.3.1 *("the organisation has a patch management procedure that enables security patches to be applied at the operating system, database, application and infrastructure levels")*, the assessment approach step does not only include a desktop review of the organisation's vulnerability management process, but a review of patching schedules for a sample of endpoints, including servers.

**The content of this framework is intended to act as a guide, outlining how evidence items could be tested. However, there are other ways of testing some of the evidence items and independent assessors should be able to do so, based on their professional judgement and knowledge of the organisation being assessed.**

Details on how the observations against each evidence item should be risk assessed, and translated into findings in the report, are outlined in the DSP Toolkit Independent Assessment Guide.

# DSP Toolkit Independent Assessment Framework - Introduction

The DSP Toolkit is designed to be applicable to **four** different categories of Health and Social Care organisation. **The categories reflect the nature of the organisations' data security and protection requirements; the volume and sensitivity of patient data processed; regulatory requirements and the relevant resilience and availability requirements** (e.g. for Operators of Essential Services or Digital Service Providers under the NIS Directive).

More DSP Toolkit assertions and evidence items are mandatory for category 2 organisations. The types of organisation in this category is shown in the table below. The DSP Toolkit Independent Assessment Framework and associated guidance has been designed this year is focused on category 2 organisations.

**Category 2**

- Independent Sector Operators of Essential Services (OES)
- IT Suppliers

# Using professional judgement

The DSPT Independent Assessment Guide (including the DSP Toolkit Strengthening Assurance Framework and associated “Big Picture Guides” ) are not exhaustive. Collectively these documents will not cover every eventuality and **professional judgement will be required** in how the standard is met and audited.

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

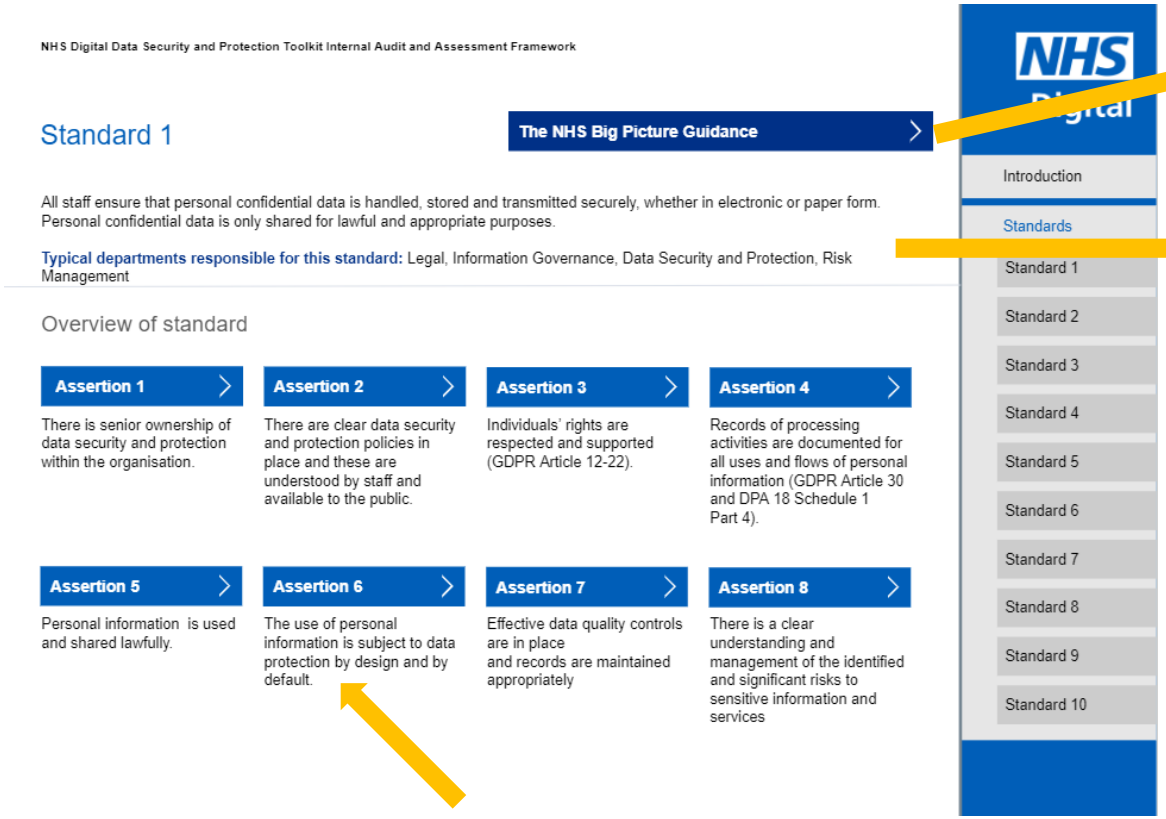
The required standards have to be achievable by those whose digital maturity is “still developing”. As a consequence, some of the measures outlined could be seen as quite manual or basic in nature. This does not mean that more sophisticated measures cannot be implemented.

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

When implementing or auditing please pay regard to the intent of the evidence, assertions, standards and ultimately the whole 10 National Data Guardian Data Security Standards. It is not the intention of the DSP Toolkit Strengthening Assurance Framework to create tick lists of items to be implemented and audited that do not reflect actual practice.

# DSP Toolkit Independent Assessment Framework - How to navigate the framework *cont.*

1. Select the relevant standard from the banner on the right-hand side of the page, Revealing the standard overview page:



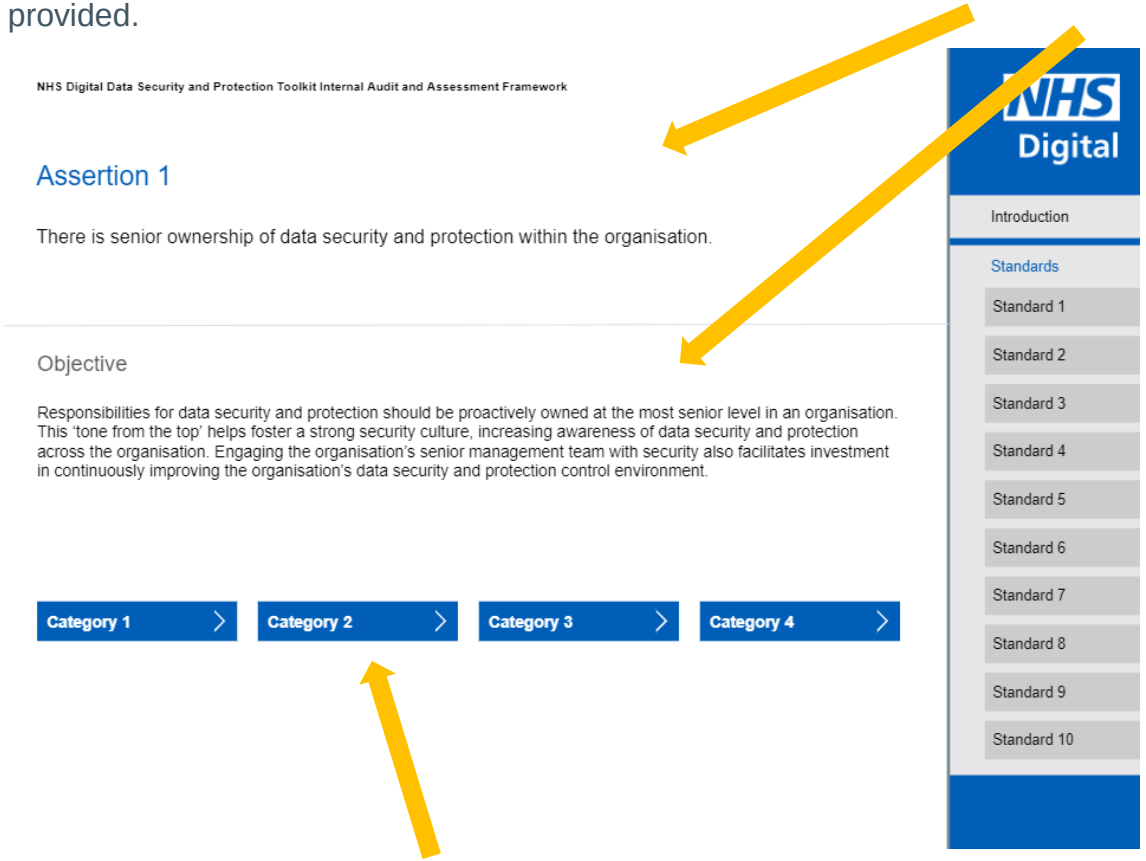

Link to external guidance/resources

Standard overview including typical departments responsible for the standard. This should give the auditor or assessor an indication of the individuals to meet with to test the evidence items in the standard.

2. Clicking on one of the assertions in the standard opens the assertion page.

# DSP Toolkit Independent Assessment Framework - How to navigate the framework *cont.*

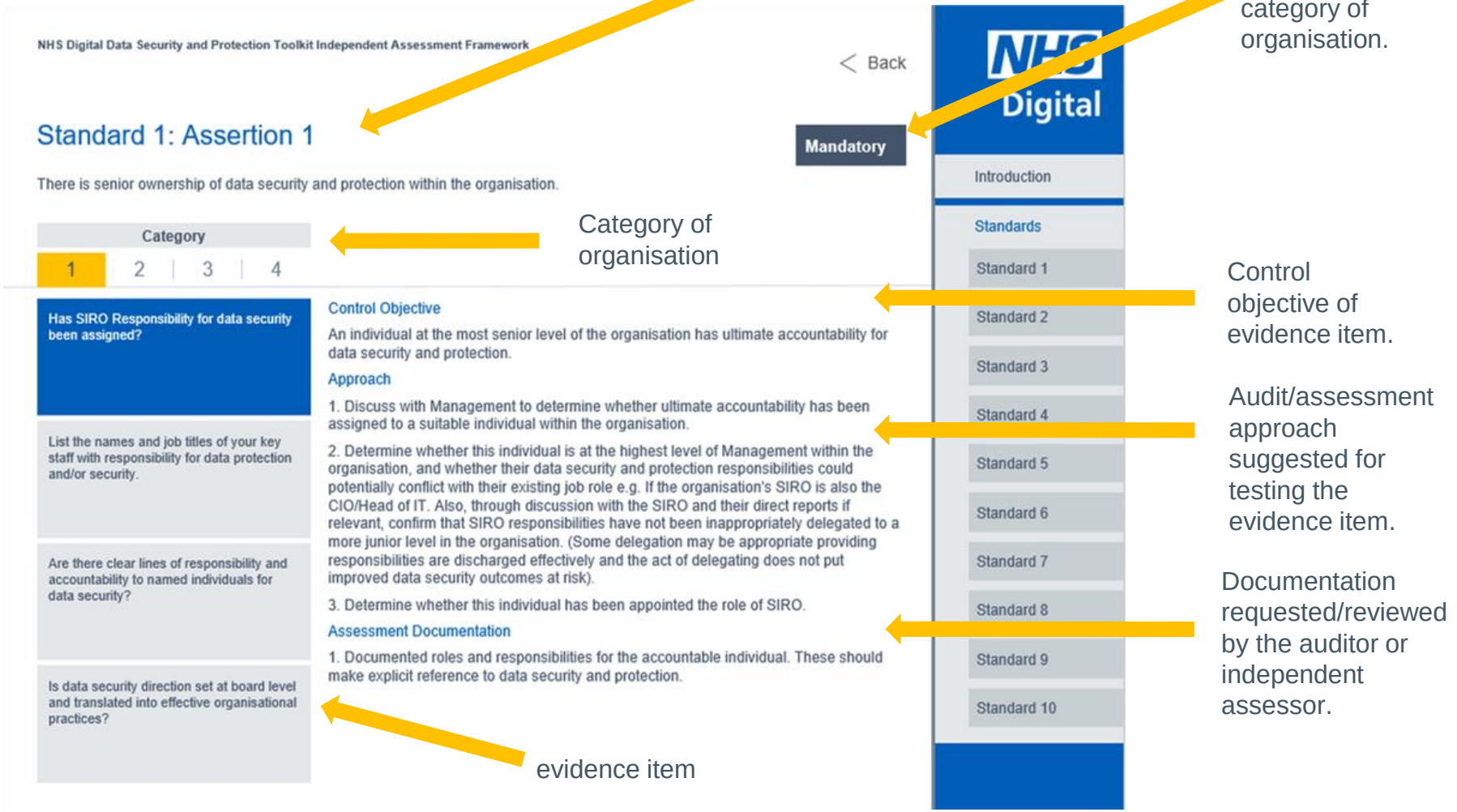
3. Please see an example assertion overview page below. The title and overarching objective of each assertion is provided.




4. Clicking on one of the categories presents the evidence item page.

# DSP Toolkit Independent Assessment Framework - How to navigate the framework *cont.*

5. Please see an example evidence item page below.



# NHS England Data Security and Protection Toolkit Independent Assessment Framework

Information and technology
for better health and care

# Standard 1 - Personal Confidential Data

The NHS Big Picture Guidance

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.
**Typical departments responsible for this standard:** Legal, Information Governance, Data Security and Protection, Risk Management.

## Overview of standard

**Assertion 1**

The organisation has a framework in place to support Lawfulness, Fairness and Transparency

**Assertion 2**

Individuals' rights are respected and supported

**Assertion 3**

Accountability and Governance in place for data protection and data security

**Assertion 4**

Records are maintained appropriately

Back

# Standard 1: Assertion 1

The organisation has a framework in place to support Lawfulness, Fairness and Transparency.

## Objective

Responsibilities for data security and protection should be proactively owned at the most senior level in an organisation. This ‘tone from the top’ helps foster a strong security culture, increasing awareness of data security and protection across the organisation. Engaging the organisation’s senior management team with security also facilitates investment in continuously improving the organisation’s data security and protection control environment.

**Category 2**

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 1: Assertion 1

## Evidence Item 1.1.1

The organisation has a framework in place to support Lawfulness, Fairness and Transparency.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

State your organisation's Information Commissioner's Office (ICO) registration number.

Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.

Transparency information (e.g. your Privacy Notice and Rights for individuals) is published and available to the public.

Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.

List the names and job titles of your key staff with responsibility for data protection and/or security

Your organisation has reviewed how you ask for and record consent.

Data quality metrics and reports are used to assess and improve data quality.

A data quality forum monitors the effectiveness of data quality assurance processes.

### Control Objective

The organisation has paid the required fee to the Information Commissioner's Office (ICO). The organisation has provided the details of its Data Protection Officer (DPO) to the ICO if this position is required under the GDPR.

### Approach

1. If it has not already been included within the organisation's most recent DSP Toolkit submission, request from the organisation their Registration Number.

2. Search the ICO's Data Protection Register: https://ico.org.uk/ESDWebPages/Search

3. Confirm that the organisation has a valid registration that is within the registration expiry date.

4. Confirm that the organisation has named their Data Protection Officer. (Categories One, Two and Four i.e. this will apply to all Public Authorities).

5. Confirm that the organisation has named their Data Protection Officer unless the organisation confirms that they have assessed a Data Protection Officer is not required under the GDPR (Category Three i.e. certain private sector organisations may conclude that they do not require a DPO).

### Assessment Documentation

1. Link to the organisation's registration page on the ICO's Data Protection Register.

Back

# Standard 1: Assertion 1

## Evidence Item 1.1.2

The organisation has a framework in place to support Lawfulness, Fairness and Transparency

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

State your organisation's Information Commissioner's Office (ICO) registration number.

Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.

Transparency information (e.g. your Privacy Notice and Rights for individuals) is published and available to the public.

Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.

List the names and job titles of your key staff with responsibility for data protection and/or security

Your organisation has reviewed how you ask for and record consent.

Data quality metrics and reports are used to assess and improve data quality.

A data quality forum monitors the effectiveness of data quality assurance processes.

### Control Objective

The organisation is able to demonstrate it has a record or register of processing that meets the requirements as laid out in the GDPR.

### Approach

1. Request to see a copy of the organisation's record of processing/Article 30 register.

2. Request to see evidence that demonstrates how the organisation has gained assurance that the record of processing includes all of the organisation's processing activities that involve personal data. The complexity of the organisation's records of processing activities will be dependent on the amount and nature of the data processed.

3. Take a sample of purposes of processing from the records of processing and confirm that the information required to meet the GDPR requirements is recorded for each of these purposes. Please refer to the Data Security and Protection (DSP) Toolkit Independent Assessment Guide.

4. Confirm that the record of processing is updated for all new/changes to processing activities involving personal data that the organisation undertakes. Review any process documentation that demonstrates how the register is reviewed and/or updated.

5. Review the organisation's DPIA process and any data mapping process to confirm that any new/changes to the processing of personal data identified through these processes triggers an update/review of the record of processing.

Continued

Back

# Standard 1: Assertion 1

## Evidence Item 1.1.2

The organisation has a framework in place to support Lawfulness, Fairness and Transparency.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

State your organisation's Information Commissioner's Office (ICO) registration number.

Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.

Transparency information (e.g. your Privacy Notice and Rights for individuals) is published and available to the public.

Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.

List the names and job titles of your key staff with responsibility for data protection and/or security

Your organisation has reviewed how you ask for and record consent.

Data quality metrics and reports are used to assess and improve data quality.

A data quality forum monitors the effectiveness of data quality assurance processes.

### Approach Continued

6. Confirm that the record of processing is reviewed on a regular basis to ensure that it is accurate and up to date. Review any process documentation that demonstrates a fixed schedule of review and that confirms that a review has taken place within the identified timescale.

7. Confirm that the organisation is in a position to provide the supervisory authority with a copy of the record of processing if it is requested to do so.

### Assessment Documentation

1. Copy of records of processing/Article 30 register.

2. Documented evidence that demonstrates how the organisation has gained assurance that the record of processing activities contains all of the organisation's processing activities that involve personal data.

3. Any process documentation that demonstrates that the records of processing activities is updated on a regular basis.

4. DPIA policy, data mapping policy and any other related policies or flow processes that demonstrate the record of processing activities is updated and/or reviewed when there is a new or changed processing activity involving personal data.

Previous

# Standard 1: Assertion 1

## Evidence Item 1.1.3

The organisation has a framework in place to support Lawfulness, Fairness and Transparency.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

State your organisation's Information Commissioner's Office (ICO) registration number.

Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.

**Transparency information (e.g. your Privacy Notice and Rights for individuals) is published and available to the public.**

Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.

List the names and job titles of your key staff with responsibility for data protection and/or security

Your organisation has reviewed how you ask for and record consent.

Data quality metrics and reports are used to assess and improve data quality.

A data quality forum monitors the effectiveness of data quality assurance processes.

### Control Objective

The organisation is informing individuals about how it is processing personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular when the information is provided to a child.

### Approach

1. Request a link to, and/or copy of; the privacy notices used by the organisation to inform patients and members of the public about how their data is processed.

2. For electronic copies of the privacy notice, request a link to the document and check that it is held in a suitably prominent position on any webpage or other public facing interfaces.

3. For paper/hard copies of the privacy notice, confirm how the notices are made publicly available. Check that the privacy notice is made clearly available to individuals. Perform three such checks.

4. Confirm that the privacy notices are made available to individuals in a timely way:

*(a)* *Where personal data is collected directly from the individual:* confirm that the privacy notices are made available to the individual at the time their personal data is collected. Test three examples given to confirm that this is the case.

Continued

# Standard 1: Assertion 1

## Evidence Item 1.1.3

The organisation has a framework in place to support Lawfulness, Fairness and Transparency.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

State your organisation's Information Commissioner's Office (ICO) registration number.

Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.

**Transparency information (e.g. your Privacy Notice and Rights for individuals) is published and available to the public.**

Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.

List the names and job titles of your key staff with responsibility for data protection and/or security

Your organisation has reviewed how you ask for and record consent.

Data quality metrics and reports are used to assess and improve data quality.

A data quality forum monitors the effectiveness of data quality assurance processes.

### Approach (cont.)

(b). *Where personal data has not been collected directly from the individual* i.e. it has been collected from a third party: confirm that the privacy notices are made available to the individual within one month of the data being collected. Test three examples given to confirm that this is the case.

5. Confirm if the organisation is processing information in relation to children. If this is the case, confirm that they are providing privacy information in a way that a child can easily understand. Review one example of a privacy notice provided where information is being processed about children to confirm that a child would reasonably be able to understand the information provided.

6. Confirm that, where requested, information can be provided to individuals orally. Take one example of a privacy notice and confirm the process for how an individual would make a request to receive the information orally and, how the organisation would facilitate this request.

7. Review one of the privacy notices provided to ensure that it provides all of the necessary information as laid out in the GDPR. Please refer to the Data Security and Protection (DSP) Toolkit Independent Assessment Guide.

### Assessment Documentation

1. Copy of or links to the privacy notices used by the organisation, including any privacy notices written specifically for children.

2. Process for providing privacy notices to individuals orally if requested (if available).

Previous

# Standard 1: Assertion 1

## Evidence Item 1.1.4

The organisation has a framework in place to support Lawfulness, Fairness and Transparency.

**Mandatory**

| Category |
| --- |
| 2 |

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

- State your organisation's Information Commissioner's Office (ICO) registration number.
- Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.
- Transparency information (e.g. your Privacy Notice and Rights for individuals) is published and available to the public.
- **Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.**
- List the names and job titles of your key staff with responsibility for data protection and/or security
- Your organisation has reviewed how you ask for and record consent.
- Data quality metrics and reports are used to assess and improve data quality.
- A data quality forum monitors the effectiveness of data quality assurance processes.

### Control Objective

The organisation understands what hardware and software assets it has and there ownership

### Approach

1. Requests to see hardware and software asset registers.
2. Determine if they are comprehensive and whether they have a valid assigned owner for them.
3. Determine if they are regularly updated and reviewed by the SIRO (or equivalent) since 1st July 2023.

Continued

# Standard 1: Assertion 1

## Evidence Item 1.1.4

The organisation has a framework in place to support Lawfulness, Fairness and Transparency.

Mandatory

| Category |
| --- |
| 2 |

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

State your organisation's Information Commissioner's Office (ICO) registration number.

Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.

Transparency information (e.g. your Privacy Notice and Rights for individuals) is published and available to the public.

**Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.**

List the names and job titles of your key staff with responsibility for data protection and/or security

Your organisation has reviewed how you ask for and record consent.

Data quality metrics and reports are used to assess and improve data quality.

A data quality forum monitors the effectiveness of data quality assurance processes.

### Assessment Documentation

~~1~~. Inventory of assets (including all third party managed assets) with recorded log of any changes, updates and reviews.

Previous

Back

# Standard 1: Assertion 1

## Evidence Item 1.1.5

The organisation has a framework in place to support Lawfulness, Fairness and Transparency.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

State your organisation's Information Commissioner's Office (ICO) registration number.

Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.

Transparency information (e.g. your Privacy Notice and Rights for individuals) is published and available to the public.

Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.

**List the names and job titles of your key staff with responsibility for data protection and/or security**

Your organisation has reviewed how you ask for and record consent.

Data quality metrics and reports are used to assess and improve data quality.

A data quality forum monitors the effectiveness of data quality assurance processes.

### Control Objective

The organisation has a data security and data protection team with the scale and capability appropriate for the size of the organisation. Job descriptions and responsibilities for these individuals are formally documented.

### Approach

1. Through discussion, or review of a documented governance/organisation structure for data security and data protection, determine whether the scale and capability of the data security and protection team appears to be appropriate for the size of the organisation and their data security risk and threat profile. This should consider whether roles/responsibilities are shared, and whether this is appropriate or presents a conflict of interest. For example, if the organisation's DPO was also the CIO/Head of IT.

2. Review this data security and protection organisation structure (if applicable), and pick a sample of individuals to assess whether they have formally documented roles and responsibilities for data security and data protection and test whether they understand their roles. If the organisation does not have an organisational structure / chart, select a sample of individuals that are known to have responsibility for data security and protection and either review their job descriptions or ask them to explain or 'draw out' the structure and describe how responsibilities for data security and protection are discharged across a group of people working together on this agenda.

### Assessment Documentation

1. Data security and data protection organisation/governance structure.

2. Documented roles and responsibilities that make reference to data security and data protection.

Back

# Standard 1: Assertion 1

## Evidence Item 1.1.6

The organisation has a framework in place to support Lawfulness, Fairness and Transparency.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

State your organisation's Information Commissioner's Office (ICO) registration number.

Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.

Transparency information (e.g. your Privacy Notice and Rights for individuals) is published and available to the public.

Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.

List the names and job titles of your key staff with responsibility for data protection and/or security

**Your organisation has reviewed how you ask for and record consent.**

Data quality metrics and reports are used to assess and improve data quality.

A data quality forum monitors the effectiveness of data quality assurance processes.

### Control Objective

The organisation has a clearly documented procedure and system to record processing which is undertaken based on the consent of an individual. The organisation is able to demonstrate that it monitors, and refreshes consent and records are kept in line with ICO guidance, to demonstrate who consented, when they consented, what they were told at the time, how they consented and whether they have withdrawn consent and if so, when. The approach to consent should be an ongoing process with choice and control and not just a one-off box ticking exercise.

### Approach

1.Through discussion, or and review of a documented process / system for recording consent, ensuring consent is monitored and refreshed and determine whether the scale and capability of the consent management

2. Review the consent procedure / policy to determine if it covers the full consent lifecycle management in line with ICO guidance https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/#how4

3. Review the system for recording consent, seeking examples that cover initial giving, reviewing and withdrawal.

### Assessment Documentation

1. The consent policy or procedure
2. The system used to record the consent management lifecycle.

Back

# Standard 1: Assertion 1

## Evidence Item 1.1.7

The organisation has a framework in place to support Lawfulness, Fairness and Transparency.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

State your organisation's Information Commissioner's Office (ICO) registration number.

Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.

Transparency information (e.g. your Privacy Notice and Rights for individuals) is published and available to the public.

Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.

List the names and job titles of your key staff with responsibility for data protection and/or security

Your organisation has reviewed how you ask for and record consent.

**Data quality metrics and reports are used to assess and improve data quality.**

A data quality forum monitors the effectiveness of data quality assurance processes.

### Control Objective

The organisation reports on the effectiveness of its data quality controls on a regular basis, enabling the continuous improvement of its data quality control environment.

### Approach

1. Discuss with Management how the organisation assesses and reports on its data quality control environment. Review a sample of any such reports.

2. Review the organisation's most recent data quality audit report and confirm that it was completed in the previous 12 months and that recommendations/actions arising from data quality reports are either being progressed or have been actioned.

### Assessment Documentation

1. Sample of data quality reports

Back

# Standard 1: Assertion 1

## Evidence Item 1.1.8

The organisation has a framework in place to support Lawfulness, Fairness and Transparency.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

State your organisation's Information Commissioner's Office (ICO) registration number.

Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.

Transparency information (e.g. your Privacy Notice and Rights for individuals) is published and available to the public.

Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.

List the names and job titles of your key staff with responsibility for data protection and/or security

Your organisation has reviewed how you ask for and record consent.

Data quality metrics and reports are used to assess and improve data quality.

A data quality forum monitors the effectiveness of data quality assurance processes.

### Control Objective

The organisation has a body or person responsible and accountable that monitors the effectiveness of its data quality control environment, and is responsible for driving data quality improvements across the organisation.

### Approach

1. Determine whether the organisation has a body or person with responsibility for data quality.

2. Request the terms of reference for the body or role description for the person concerned and determine whether its membership / activities includes individuals from across the organisation, and whether the roles, responsibilities and reporting lines to/from the body / person concerned are defined.

3. Request and review a sample of the body's minutes.

### Assessment Documentation

1. Data quality forum terms of reference.

2. Sample of data quality forum minutes.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 1: Assertion 2

Individuals' rights are respected and supported

## Objective

Having a suite of data security and protection policies and procedures, which are updated regularly and in line with industry good practice, enables security controls to be applied consistently across an organisation. They can also be a mechanism for raising staff awareness on security, informing them of their responsibilities in maintaining the organisation's data security and protection control environment.

**Category 2**

# Standard 1: Assertion 2

## Evidence Item 1.2.2

There is senior ownership of data security and protection within the organisation.

**Mandatory**

| Category |
| --- |
| 2 |

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

**Your organisation has processes in place to deliver individuals rights including to handle an individual's objection to the processing of their personal data.**

Your organisation has a process to recognise and respond to individuals' requests to access their personal data.

Your organisation is compliant with the national data opt-out policy.

### Control Objective

The organisation is able to recognise and respond to an individual's request to object to the processing of their personal data.

### Approach

1. Through discussion understand the organisation's approach to handling objection requests
2. Review the organisation's procedure on how to handle individual's objection to processing and confirm compliance with ICO guidance https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/
3. Request to review a sample of cases where an individual objected to their data being processed and check for compliance.

### Assessment Documentation

1. The organisation's procedure on handling requests from individuals objecting to their data being processed.
2. Evidence that the procedure has been applied appropriately.

# Standard 1: Assertion 2

## Evidence Item 1.2.3

There is senior ownership of data security and protection within the organisation.

Mandatory

**Category**

2

Your organisation has processes in place to deliver individuals rights including to handle an individual's objection to the processing of their personal data.

**Your organisation has a process to recognise and respond to individuals' requests to access their personal data.**

Your organisation is compliant with the national data opt-out policy.

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

### Control Objective

The organisation has policies and procedures in place that illustrate how to recognise and respond to an individual's request to access their personal data.

### Approach

1. Review the organisation's SARs policies and procedures, confirming they include how to recognise and respond to SARs, including when restrictions may apply, in line with ICO guidance.

2. Confirm with recent examples how requests have been responded to and where appropriate an exemption has been applied.

### Assessment Documentation

1. SAR policies and procedures
2. Evidence that a randomly selected set of SAR requests have been dealt with appropriately

# Standard 1: Assertion 2

## Evidence Item 1.2.4

There is senior ownership of data security and protection within the organisation.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation has processes in place to deliver individuals rights including to handle an individual's objection to the processing of their personal data.

Your organisation has a process to recognise and respond to individuals' requests to access their personal data.

Your organisation is compliant with the national data opt-out policy.

### Control Objective

The organisation is able to demonstrate compliance with the National Data Opt-out Policy.

### Approach

1. Request to see evidence of the documented procedures that the organisation has in place to comply with the data opt-out policy.

2. Request to see evidence that the organisation has implemented a technical solution to enable them to check lists of NHS numbers against national data opt-outs registered.

3. Request to see evidence that the process and documented procedures have been approved by the organisation's board or an appropriate committee or group with senior management membership.

4. Request to see evidence that there is a process in place to test that the technical solution and process is working in a business as usual environment.

5. Request to see evidence of any actual testing undertaken to ensure that the technical solution and process is working in a business as usual environment.

### Assessment Documentation

1. Procedures outlining how the organisation will comply with the data opt-out policy.

2. Evidence that the organisation has implemented a technical solution to enable them to check lists of NHS numbers against those with national data opt-outs registered.

3. Board or committee/meeting minutes that demonstrate the procedure has been formally approved.

4. Policy or process documentation that lay out how compliance with the opt-out policy will be tested and evidence of any testing that has been undertaken. i.e. comfort that those who have opted out will not have their data inappropriately processed without consent.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 1: Assertion 3

Accountability and Governance in place for data protection and data security

## Objective

The organisation has policies and processes in place to fulfil the rights of data subjects under the General Data Protection Regulation (GDPR). These rights include;

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

**Category 2**

Back

# Standard 1: Assertion 3

## Evidence Item 1.3.1

Accountability and Governance in place for data protection and data security

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

There are board-approved data security and protection policies in place that follow relevant guidance.

Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.

SIRO responsibility for data security has been assigned.

There are clear documented lines of responsibility and accountability to named individuals for data security and data protection.

Your organisation operates and maintains a data security and protection risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility.

List your organisation’s top three data security and protection risks.

1.3 Continued

### Control Objective

The organisation has a suite of data security and data protection policies and procedures that are approved at the Board level.

### Approach

1. Review the organisation's data security and data protection policies and procedures, confirming they include: Data protection, data quality, records management, data security, registration authority, Subject Access Requests, Freedom of Information and network security.

2. For category 1 organisations, review a sample of the policies/procedures and confirm whether they have been approved by the organisation's Board. For category 3 and 4 organisations, confirm that they have been approved by an appropriate individual/body.

### Assessment Documentation

1. Relevant data security and data protection policies and procedures.

2. Evidence that a sample of the policies and procedures have been approved by an appropriate individual/body.

# Standard 1: Assertion 3

## Evidence Item 1.3.2

Accountability and Governance in place for data protection and data security

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

There are board-approved data security and protection policies in place that follow relevant guidance.

**Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.**

SIRO responsibility for data security has been assigned.

There are clear documented lines of responsibility and accountability to named individuals for data security and data protection.

Your organisation operates and maintains a data security and protection risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility.

List your organisation's top three data security and protection risks.

1.3 Continued

### Control Objective

Organisations are undertaking regular testing and quality assurance to ensure that staff are following the requirements in practice as laid out in their guidance and policies and procedures in relation to Data Protection and Confidentiality.

### Approach

1. Does the organisation undertake any spot checks / formal testing to assess whether staff are complying with Data Protection/Confidentiality guidance and/or policies and procedures in practice? Request to review evidence to support this assertion.

2. Request to review a copy of any action plan that has resulted from the testing being undertaken.

3. Does the action plan (or similar) outline clear actions with timescales for completion, responsibilities for who has approved an action and who has responsibility for completing it? Review evidence to support this assertion.

4. When on-site, with the relevant member of the Data Security and Protection team, request to observe evidence associated with a sample of actions being implemented. For example, where additional training/awareness materials have been produced e.g. Posters/screensavers, request to view them / be shown them in the office space.

5. Is the action plan regularly reviewed by an appropriate board, committee, meeting or group of the organisation that has representation from senior management? Review evidence to support this assertion.

Continued

Back

# Standard 1: Assertion 3

## Evidence Item 1.3.2

Accountability and Governance in place for data protection and data security

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

There are board-approved data security and protection policies in place that follow relevant guidance.

Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.

SIRO responsibility for data security has been assigned.

There are clear documented lines of responsibility and accountability to named individuals for data security and data protection.

Your organisation operates and maintains a data security and protection risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility.

List your organisation's top three data security and protection risks.

1.3 Continued

6. Is there a clear follow up/escalation process to identify and act on any actions not completed within the required timescales? Review evidence to support this assertion.

### Assessment Documentation

1. Testing programme or documentation to evidence there is a formal process in place to provide assurance that staff are complying with the relevant guidance and/or policies and procedures. Results of spot checks

2. Copy of action plan that has resulted from any testing having been undertaken.

3. Evidence that the action plan has been reviewed by an appropriate board, committee, meeting or group of the organisation that has representation from senior management.

4. Evidence associated with actions being implemented, for example, additional training/awareness materials that have been produced e.g. Posters/screensavers.

Previous

Back

# Standard 1: Assertion 3

## Evidence Item 1.3.3

Accountability and Governance in place for data protection and data security

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

There are board-approved data security and protection policies in place that follow relevant guidance.

Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.

SIRO responsibility for data security has been assigned.

There are clear documented lines of responsibility and accountability to named individuals for data security and data protection.

Your organisation operates and maintains a data security and protection risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility.

List your organisation's top three data security and protection risks.

1.3 Continued

### Control Objective

An individual at the most senior level of the organisation has ultimate accountability for data security and protection.

### Approach

1. Discuss with Management to determine whether ultimate accountability has been assigned to a suitable individual within the organisation.

2. Determine whether this individual is at the highest level of Management within the organisation, and whether their data security and protection responsibilities could potentially conflict with their existing job role e.g. If the organisation's SIRO is also the CIO/Head of IT. Also, through discussion with the SIRO and their direct reports if relevant, confirm that SIRO responsibilities have not been inappropriately delegated to a more junior level in the organisation. (Some delegation may be appropriate providing responsibilities are discharged effectively and the act of delegating does not put improved data security outcomes at risk).

3. Determine whether this individual has been appointed the role of SIRO.

### Assessment Documentation

1. Documented roles and responsibilities for the accountable individual. These should make explicit reference to data security and protection.

Back

# Standard 1: Assertion 3

## Evidence Item 1.3.4

Accountability and Governance in place for data protection and data security

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

There are board-approved data security and protection policies in place that follow relevant guidance.

Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.

SIRO responsibility for data security has been assigned.

**There are clear documented lines of responsibility and accountability to named individuals for data security and data protection.**

Your organisation operates and maintains a data security and protection risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility.

List your organisation's top three data security and protection risks.

1.3 Continued

### Control Objective

The organisation has a clearly documented governance/organisation structure for those individuals that have responsibility for data security and data protection. This includes clear lines of reporting, responsibility and accountability to a senior level of Management.

### Approach

1. Request and review the organisation's data security and data protection governance structure(s).

2. Review this governance structure and determine if it includes clear lines of responsibility and accountability from the data security and data protection operational team(s) to a senior level of Management.

3. Ask a member of the DSP team to walk through the organisation's Data Security and Protection governance structure, including how they ultimately report into the Head of DSP and/or the SIRO.

### Assessment Documentation

1. Formally documented reporting for individuals with responsibility for data security and data protection.

# Standard 1: Assertion 3

## Evidence Item 1.3.5

Accountability and Governance in place for data protection and data security

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

There are board-approved data security and protection policies in place that follow relevant guidance.

Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.

SIRO responsibility for data security has been assigned.

There are clear documented lines of responsibility and accountability to named individuals for data security and data protection.

**Your organisation operates and maintains a data security and protection risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility.**

List your organisation's top three data security and protection risks.

1.3 Continued

### Control Objective

The organisation effectively identifies, manages and mitigates risks relating to data security and data protection, and records and tracks any mitigating controls/actions in place, linking in with organisation wide approaches to risk management.

### Approach

1. Review the organisation's data security and data protection risk register. Confirm that it has been reviewed and updated in the previous 12 months, and is aligned to the National Cyber Security Centre's (NCSC) guidance on information risk management. Please see https://www.ncsc.gov.uk/guidance/summary-risk-methods-and-frameworks for more guidance.

2. Review the content of the register and assess whether it contains risks specific to the organisation, that the risks are assessed appropriately, and that mitigating controls/actions have been assigned to each risk. Understand how these controls/actions are managed and that they include target dates for implementation with senior ownership.

3. By reviewing/comparing the organisation's data security and data protection and corporate risk frameworks, determine whether the two are aligned and understand how reporting/escalation of data security and data protection risks is managed and review associated evidence. Confirm that data security and data protection-related risks are included on the organisation's corporate/overarching risk register.

Continued

Back

# Standard 1: Assertion 3

## Evidence Item 1.3.5

Accountability and Governance in place for data protection and data security

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

There are board-approved data security and protection policies in place that follow relevant guidance.

Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.

SIRO responsibility for data security has been assigned.

There are clear documented lines of responsibility and accountability to named individuals for data security and data protection.

**Your organisation operates and maintains a data security and protection risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility.**

List your organisation's top three data security and protection risks.

1.3 Continued

### Approach (continued)

4. Determine if the governance of data security risk management extends to the supply chain, particularly for critical suppliers/vendors. This should include identification and management of suppliers/vendors, on/off-boarding and compliance management, and integrated cyber security incident response and recovery testing.

### Assessment Documentation

1. Data security and protection risk management framework and risk register.
2. Corporate risk management framework and risk register.
3. Evidence associated with data security and protection risks being reported/escalated.
4. Third party security assessment process and policy. Third party audit reports and template contracts.

Previous

Back

# Standard 1: Assertion 3

## Evidence Item 1.3.6

Accountability and Governance in place for data protection and data security

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

There are board-approved data security and protection policies in place that follow relevant guidance.

Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.

SIRO responsibility for data security has been assigned.

There are clear documented lines of responsibility and accountability to named individuals for data security and data protection.

Your organisation operates and maintains a data security and protection risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility.

List your organisation's top three data security and protection risks.

1.3 Continued

### Control Objective

The organisation has a mechanism for assessing/prioritising data security and data protection risks, based on the likelihood of the risk crystallising into an issue, and the impact if it did.

### Approach

1. Review the organisation's data security and data protection risk management framework, confirming that it contains a mechanism to assess risks based on likelihood and impact.

2. Review the risk assessment associated with the organisation's top 3 data security and data protection risks, confirming that they were assessed in line with the overarching framework.

3. Through discussion with the relevant individual in the Data Security and Protection team, understand how frequently these risks (top 3 and remainder) are reviewed and updated. For example, if the top 3 risks have not changed in a number of years, it could be a sign that the organisation is not fully engaged, regularly enough; in data security and protection risk management, where the external threat environment evolves rapidly.

4. Understand who is responsible for carrying out the data security and protection risk assessments. Confirm that they have the knowledge and capability to assess these risks. Also walk through how data security and protection risks are reported to a senior level in the organisation for oversight and/or approval.

5. From the independent assessor's / auditor's understanding of the organisation and industry, confirm that the top three risks that have been identified appear to be appropriate.

### Assessment Documentation

1. Data security and protection risk management framework.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 1: Assertion 3

## Evidence Item 1.3.7

Accountability and Governance in place for data protection and data security

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.

Your organisation understands when you must conduct a DPIA and has processes in place, which links to your existing risk management and project management, to action this.

Data security and protection direction is set at board level and translated into effective organisational practices.

1.3 Previous

### Control Objective

The organisation has a clear procedure that sets out how it will implement data protection by design and default within organisational practices that involve the processing of personal data. The organisation has a clear procedure for pseudonymisation and guidance as regards the risks of linking other data sets with anonymised or pseudonymised data sets which may inadvertently support inappropriate identification / re-identification of individuals.

### Approach

1. Request to review a copy of the organisation's procedures that lay out its approach to data protection by design and by default and to pseudonymisation.

2. Review that, at a minimum, the procedure ensures that the GDPR principles and appropriate technical and organisational measures to protect personal data, are built by default into the organisation's processing activities and business practices, from the design stage right through the lifecycle.

3. Request to review evidence that the procedure has been approved by the organisation's board or equivalent.

4. Has the organisation implemented data protection into any wider business processes, strategies and organisational vision statements to build in data protection to the heart of its organisational practice?

### Assessment Documentation

1. Copy of Data Protection by Design and Default procedure.

2. Evidence, such as minutes or a signed copy of the procedure that demonstrates it has been approved by the organisation's board (or similar).

3. Evidence of any wider practice that the organisation has built in data protection principles into any wider business processes, strategies and organisational vision statements.

# Standard 1: Assertion 3

## Evidence Item 1.3.8

Accountability and Governance in place for data protection and data security

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.

Your organisation understands when you must conduct a DPIA and has processes in place, which links to your existing risk management and project management, to action this.

Data security and protection direction is set at board level and translated into effective organisational practices.

1.3 Previous

### Control Objective

The organisation has a procedure in place for carrying out Data Protection Impact Assessments that meets legal and regulatory requirements and helps drive improvements in privacy and data protection.

### Approach

1. Request to review a copy of the organisation's Data Protection Impact Assessment procedure (or similar document).

2. Confirm that the procedure has been approved by the organisation's SIRO

3. Confirm that the procedure meets the requirements as laid out in the GDPR and guidance issued by the regulator. Please refer to the Data Security and Protection (DSP) Toolkit Independent Assessment Guide.

4. Confirm that the procedure has been approved by the organisation's board (or similar) and is scheduled for review at least on a biennial basis (every 2 years).

### Assessment Documentation

1. Data Protection Impact Assessment Procedure (or similar).

2. Evidence that the procedure has been approved by the SIRO or the individual with responsibility for data security/data protection.

3. Evidence that the procedure has been approved by the organisation's board (or similar) and is scheduled for review at least on a biennial basis.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 1: Assertion 3

## Evidence Item 1.3.9

Accountability and Governance in place for data protection and data security

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.

Your organisation understands when you must conduct a DPIA and has processes in place, which links to your existing risk management and project management, to action this.

Data security and protection direction is set at board level and translated into effective organisational practices.

1.3 Previous

### Control Objective

The highest level of Management within the organisation is responsible for setting the strategic direction for data security and data protection.

### Approach

1. Review Board agendas and minutes for the previous year and determine if data security and data protection has been discussed.

2. Determine if there is regular reporting to the Board on the effectiveness of the organisation's data security and data protection control environment.

(For category 3, Management meeting will suffice).

3. Assess the effectiveness of these reports in giving Management appropriate management information and oversight. For example, do they contain sufficient detail to enable Management to understand the risks and make strategic decisions on data security and data protection?

4. Where the organisation's highest level of Management/Board has delegated authority to another body for more regular management/oversight of Data Security and Protection, review evidence that this delegated authority has been formally documented. Also review evidence associated with this body escalating issues to the highest level of Management/Board where appropriate.

### Assessment Documentation

1. Board agenda and meeting minutes.

2. Example data security and data protection related reports.

3. Documented evidence of delegated authority to another body for the more regular management of Data Security and Protection.

4. Reports from the delegated body to the highest level of Management/Board.

Back

# Standard 1: Assertion 4

Records are maintained appropriately

## Objective

As well as being a key requirement for compliance with the GDPR, maintaining a record of processing activities gives Management oversight of its high risk instances of data processing, allowing it to take a risk-based approach when investing in security controls to secure the organisation’s most critical assets.

**Category 2**

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 1: Assertion 4

Mandatory

## Evidence Item 1.4.1

Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and DPA 18 Schedule 1 Part 4).

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

The organisation has a records management policy including a records retention schedule.

### Control Objective

The organisation has created has a records management policy covering scope, obligations and a records retention schedule that defines how long it should store the data assets under its control. This should minimise the amount of data stored by the organisation, reducing both the likelihood and impact of a data breach.

### Approach

1. Determine if the organisation has created a records management policy including a records retention schedule in line with the requirements of the Records Management Code of Practice for Health and Social Care 2020 Records Management Code of Practice 2020 (nhsx.nhs.uk).

2. Review the policy and retention schedules and determine whether a sample of the retention periods meet the minimum requirements of the NHS England guidance.

### Assessment Documentation

1. Records Management Policy

2. Record retention schedule.

# Standard 2 - Staff Responsibilities

The NHS Big Picture Guidance

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.
**Typical departments responsible for this standard:** Information Governance, Data Security and Protection and HR

## Overview of standard

**Assertion 1**

Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.

**Assertion 2**

Staff contracts set out responsibilities for data security

Back

# Standard 2: Assertion 1

Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.

## Objective

The objective of this assertion is to raise awareness of data security and protection across the organisation, by implementing induction training for all new members of staff, including data security and protection clauses in all staff contracts, and assessing staff awareness on data security and protection.

**Category 2**

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 2: Assertion 1

## Evidence Item 2.1.1

Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

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

### Control Objective

Data security and data protection are included as part of the induction process to ensure that all new joiners are aware of the importance of data security and data protection, and are made aware of their responsibilities in these areas.

### Approach

1. Obtain evidence that the organisation is a member of the Cyber Associates Network e.g. Confirmation email.

### Assessment Documentation

1. Email confirming that the organisation is a membership of the Cyber Associates Network.

Back

# Standard 2: Assertion 2

## Staff contracts set out responsibilities for data security

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

## Objective

The objective of this assertion is to ensure that staff contracts contain appropriate data security and protections requirements.

**Category 2**

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 2: Assertion 2

## Evidence Item 2.2.1

Staff contracts set out responsibilities for data security

**Mandatory**

**Category**

2

All employment contracts contain data security requirements.

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

### Control Objective

All staff are contractually obligated to take personal responsibility for data security and data protection.

### Approach

1. Through discussion with Management, determine if responsibility for data security and data protection is addressed appropriately in staff contracts. Request and review the standard/model employment contract and determine if the clauses are included as described. These should go beyond confidentiality agreements and include, for example, requirements to follow the relevant IT security policies and procedures.

### Assessment Documentation

1. Standard contract template (or extract) including data security requirements.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 3 - Training

The NHS Big Picture Guidance

All staff have an appropriate understanding of information governance and cyber security. Organisations have more flexibility to set local training requirements that are proportionate to different staff roles, and to adopt a range of different methods to deliver that training. However, the approach will need to be proportionate to the size and type of organisation.

**Typical departments responsible for this standard:** Information Governance, Data Security and Protection, HR

## Overview of standard

### Assertion 1

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

### Assertion 2

Your organisation engages proactively and widely to improve data security and has an open and just culture for data security incidents.

# Standard 3: Assertion 1

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

## Objective

Understanding the data security and protection training needs of its staff, based on their role and access to confidential data, allows an organisation to identify gaps in training/capability. It can then create an action plan to fill these gaps, upskilling staff where necessary.

**Category 2**

# Standard 3: Assertion 1

## Evidence Item 3.1.1

There has been an assessment of data security and protection training needs across the organisation.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

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.

Your organisation's defined training and awareness activities are implemented for and followed by all staff.

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

### Control Objective

The organisation has conducted a training needs analysis to identify an appropriate level of training and awareness for different staff groups. This has been endorsed and resourced approved by senior leadership.

### Approach

1. Request and review the organisation's training needs analysis document, confirming that it includes all staff groups and was completed/reviewed in the previous 12 months.

2. Through discussion with management understand whether the training needs analysis activities are proportionate to the size and type and complexity of the organisation. This should consider the understanding required from different staff groups and the mix and coverage of awareness and training campaigns.

### Assessment Documentation

1. Training needs analysis document.

2. Evidence that the organisation's senior leadership have endorsed and resourced the training needs analysis document.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 3: Assertion 1

## Evidence Item 3.1.2

Training and awareness implementation.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

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.

Your organisation's defined training and awareness activities are implemented for and followed by all staff.

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

### Control Objective

The organisation has implemented a training needs analysis actions.

### Approach

1. From the training needs analysis document, select a sample of entries for several staff groups.

2. Confirm for that sample that the associated activities for those staff groups have been initiated (note levels of training required in that staff group may mean that staff have not received activities yet).

### Assessment Documentation

1. Training needs analysis document.

2. Evidence of TNA activities.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 3: Assertion 1

## Evidence Item 3.1.3

There has been a review of data security and protection training activities across the organisation.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

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.

Your organisation's defined training and awareness activities are implemented for and followed by all staff.

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

### Control Objective

The organisation understands the effectiveness of its training and awareness approach.

### Approach

1. Through discussion with management and the training need analysis document understand how the organisation intends to measure the effectiveness of its training and awareness approach.

2. Review those plans/intentions ensuring they are realistic and proportionate to the size and type and complexity of the organisation

### Assessment Documentation

1. Training needs analysis document.

2. Training and awareness evaluation plans

# Standard 3: Assertion 2

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

## Objective

To have an open and just culture that recognises the importance of cyber security and information governance from the most senior leaders to those at the front line. Although culture is difficult to change, a positive and engaged culture brings dividends in having a unifying understanding and appreciation in this area.

**Category 2**

# Standard 3: Assertion 2

## Evidence Item 3.2.1

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

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

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

Actions are taken openly and consistently in response to information governance and cyber security concerns.

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

### Control Objective

Cyber security and information governance matters receive proportionate priority attention by boards or equivalent senior leaders.

### Approach

1. Determine the boards or equivalent senior leader's forum

2. Request agenda items and minutes where cyber security or information governance matters feature on the agenda and associated minutes within the last 12 months.

3. Determine from those agenda items and minutes if the volume, nature and associated actions are sufficiently addressed and prioritised.

4. Determine senior leadership attendance and promotion in cyber security and information governance campaigns and events.

### Assessment Documentation

1. Board Agenda and minutes with evidence of cyber security and information governance matters being addressed.

2. Evidence of senior attendance and/or promotion at information governance and security events / campaigns.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 3: Assertion 2

## Evidence Item 3.2.2

Actions are taken openly and consistently in response to information governance and cyber security concerns.

.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

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

**Actions are taken openly and consistently in response to information governance and cyber security concerns**

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

### Control Objective

Cyber security and information governance concerns are treated in an open and transparent fashion.

### Approach

1. Through management discussion determine how the organisation handles concerns that are raised including how they are recorded and actioned.

2. From those records select a sample of raised concerns following the journey from conception through to conclusion to see that they are treated in an open and positive fashion and the outcome is used to provide a learning opportunity.

3. Where appropriate and possible contact the initiator of one of those concerns for feedback on how their concern was treated.

### Assessment Documentation

1. Records of cyber security and information governance concerns.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 3: Assertion 2

## Evidence Item 3.2.3

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

**Category**

2

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

Actions are taken openly and consistently in response to information governance and cyber security concerns.

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

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

### Control Objective

Your programme is informed and representative of the organisation it serves and is not limited to just an information governance / cyber security silo.

### Approach

1. Determine the representation within information governance and cyber security groups is representative and includes clinical representation (where appropriate to the organisation).

2. Determine how the organisation additionally seeks to inform its programme through initiatives such as champions networks, information flow registers, cyber security and information governance staff being part of wider networks and survey / interviewing staff.

### Assessment Documentation

1. Terms of references and attendance sheets of cyber and information security groups.

2. Evidence of other initiatives that help inform and spread wider engagement such as from Information assets flow and register participation.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 4 - Managing Data Access

The NHS Big Picture Guidance

Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals. The principle of 'least privilege' is applied, so that users do not have access to data they have no business need to see. Staff do not accumulate system accesses over time. User privileges are proactively managed so that there is, as far as is practicable, a forensic trail back to a specific user or user group. Where necessary, organisations will look to non-technical means of recording IT usage (e.g. sign in sheets, CCTV, correlation with other systems, shift rosters etc.).

**Typical departments responsible for this standard:** IT, IT Security, HR, Data Security and Protection

## Overview of standard

### Assertion 1

The organisation maintains a current record of staff and their roles.

### Assertion 2

The organisation assures good management and maintenance of identity and access control for its networks and information systems

### Assertion 3

All staff understand that their activities on IT systems will be monitored and recorded for security purposes.

### Assertion 4

You closely manage privileged user access to networks and information systems supporting the essential service.

### Assertion 5

You ensure your passwords are suitable for the information you are protecting.

Back

# Standard 4: Assertion 1

The organisation maintains a current record of staff and their roles.

## Objective

In order to minimise the amount of data that individuals have access to, organisations should implement the principle of least privilege - only granting users the level of access that is required for them to carry out their role. In order to support a strong access control environment, systems should only be accessed using unique login credentials.

**Category 2**

# Standard 4: Assertion 1

## Evidence Item 4.1.1

The organisation maintains a current record of staff and their roles.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation understands who has access to personal and confidential data through your systems, including any systems which do not support individual logins

Users in your organisation are only given the minimum access to sensitive information or systems necessary for their role

### Control Objective

The organisation maintains a record of all staff and their roles across the organisation. Where possible, users access the organisation's systems using unique logon credentials. Where this is not possible, it is formally documented and risk accepted.

### Approach

1. Determine if the organisation maintains a record of all staff across the organisation, and if this record is updated on a regular basis. Also f the organisation has a high-level understanding of which of its systems do not have unique user credentials. For a sample of these, determine if this has been formally risk accepted and whether a manual access list is maintained.

2. Request and review the Data Security and Protection organisation structure, confirming that it reflects the actual team in place.

3. For a sample of systems that do have unique user credentials, review the UAL while on site and confirm that there are no generic accounts. Understand if there are any mitigating controls for a sample of systems that do not have unique user credentials, for example, the system can only be accessed through a specific device or from a particular location.

4) Enquire as to plans to augment or improve authentication / Identity and Access Management / Role-Based Access Control / Privileged User Access Management (PAM). Request a spot-check whilst on-site, for a user to be picked at random to be shown systems access.

### Assessment Documentation

1 Organisation chart/organisation structure.

2. Role / Job descriptions.

3. ESR (Electronic Staff Record)

4. Overview of systems with unique user logins,

5. Risk acceptance without unique use logins.

6. Plans for authentication / IdAM / PAM.

7. Microsoft AD DS based on DNS. Note: this will not cover other systems that are not Windows.

# Standard 4: Assertion 1

## Evidence Item 4.1.2

The organisation maintains a current record of staff and their roles.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation understands who has access to personal and confidential data through your systems, including any systems which do not support individual logins

Users in your organisation are only given the minimum access to sensitive information or systems necessary for their role

### Control Objective

The organisation's access controls enforce the principle of least privilege, minimising levels of systems access to the amount that is required for each of the organisation's roles.

### Approach

1. Understand how the organisation has implemented the principle of least privilege. Review the organisation's access control policy and determine if Management's description of the control is outlined in policy.

2. If Role-based Access Control (RBAC) has been implemented, request and review the matrix that relates role to system access. Determine if, and review associated evidence, the RBAC matrix is reviewed and updated on at least an annual basis.

3. If RBAC (or similar) has been implemented, while on-site, select a sample of users and confirm that their system access (for one key system e.g. patient record) is configured as per the RBAC matrix.

### Assessment Documentation

1. Access control policy.

2. RBAC matrix, and evidence that it is regularly reviewed and updated.

3. Evidence of user system access.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 4: Assertion 2

The organisation assures good management and maintenance of identity and access control for it's networks and information systems.

## Objective

Regular user reviews, for both standard and administrator level access, is a key control in ensuring that only authorised users have access to the organisation's systems and data.

Organisations should also design and implement an effective log management framework that allows it to monitor user actions for potentially malicious or suspicious activities, and retrospectively analyse the logs to determine the root cause of security incidents.

**Category 2**

Back

# Standard 4: Assertion 2

## Evidence Item 4.2.1

The organisation assures good management and maintenance of identity and access control for its networks and information systems.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

When was the last audit of user accounts with access to the organisation's systems held?

Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted

Logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity

Unnecessary user accounts are removed or disabled

### Control Objective

Regular audits of user access are performed to ensure that access to the organisation's network is appropriate. The audit of systems should be scoped around those that contain personal confidential information as defined in this document.

### Approach

1. Discuss with Management to determine whether annual user access audits are performed.

2. Request evidence of the last user access review and determine whether it was completed within the last 12 months by an appropriate individual.

3. Request and compare the organisation's leavers list from HR, to its Active Directory (AD) user list to determine if there are any leavers that still have access to the organisation's systems. Where leavers do have access, determine if their account has been used since their leave date.

4. When on-site, walk through the organisation's process for managing Movers - individuals that have changed role within the organisation.

### Assessment Documentation

1. Evidence of the previous user access audit e.g. Signed user listing or other confirmation that the user access audit took place.

# Standard 4: Assertion 2

## Evidence Item 4.2.2

The organisation assures good management and maintenance of identity and access control for its networks and information systems.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

When was the last audit of user accounts with access to the organisation's systems held?

Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted

Logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity

Unnecessary user accounts are removed or disabled

### Control Objective

The organisation learns lessons from data security and protection incidents relating to access control and inappropriate user privileges and then implements mitigating actions to continuously improve its control environment.

### Approach

1. Request list of security incidents relating to access management issues.

2. Review list provided to determine whether the issues are related to access management issues, and determine if remediating actions have been assigned and/or implemented.

### Assessment Documentation

1. List of security incidents relating to access management issues.

2. Documented actions designed to mitigate the root cause of previous access management issues.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 4: Assertion 2

## Evidence Item 4.2.3

The organisation assures good management and maintenance of identity and access control for its networks and information systems.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

When was the last audit of user accounts with access to the organisation's systems held?

Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted

**Logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity**

Unnecessary user accounts are removed or disabled

### Control Objective

The organisation has documented a log retention policy that outlines its approach to storing the logs of authenticated users. This policy should include details on maintaining the integrity of the logs, offline backup for disaster recovery purposes, internet logs and mobile device/tablet logs.

### Approach

1. Discuss with Management to determine whether the organisation has documented a log retention policy. If in place, review the log management policy to determine whether the sections outlined in the control objective column are included.

2. Determine whether, in line with the log retention policy, logs are retained for a minimum of six months to enable their use for the detection of potential malicious activity.

3. Enquire with Management as to the processes, automated or manual, for reviewing logs to proactively or retrospectively identify any potential incidents.

4. Depending on the response to 2, review evidence associated with the control implementation. For example, if a Security Incident and Events Monitoring (SIEM) solution has been implemented to automatically review logs, reporting from the SIEM could be reviewed. If a manual log review process is in place, any associated evidence could be reviewed.

### Assessment Documentation

1. Log retention policy.
2. Documentation associated with automated or manual log review controls.

# Standard 4: Assertion 2

## Evidence Item 4.2.4

The organisation assures good management and maintenance of identity and access control for its networks and information systems.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

When was the last audit of user accounts with access to the organisation's systems held?

Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted

Logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity

Unnecessary user accounts are removed or disabled

### Control Objective

The number of unnecessary user accounts (e.g. previous guest/employee) are minimised to reduce the risk of their access being exploited.

### Approach

1. Determine if the organisation has an access management policy, or similar, that documents how access is removed from user accounts that are no longer required and whether payroll systems or other means, such as manual processes, are involved in triggering the revocation of access. Understand how the organisation identifies Leavers, including those that are on long-term absence e.g. Parental leave.

2. Select a small sample of 'leavers' and determine that their access was removed in line with the access management policy (see audit guide for sample size).

3. Discuss with the responsible individual the processes and controls for those remaining in employment but whose change of role should cause a review and possible revocation of system and data access privileges, or a subset thereof.

### Assessment Documentation

1. Access management policy or similar.

2. Evidence that, for a small sample of 'leavers', access has been removed in line with the policy.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 4: Assertion 3

All staff understand that their activities on IT systems will be monitored and recorded for security purposes.

## Objective

In order to comply with data protection regulations, organisations must make staff aware of how their IT use will be recorded and monitored for security purposes. In addition, staff should continuously be informed of their personal responsibility for maintaining the organisation's data security and protection control environment.

**Category 2**

Back

# Standard 4: Assertion 3

## Evidence Item 4.3.1

All staff understand that their activities on IT systems will be monitored and recorded for security purposes.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All system administrators have signed an agreement which holds them accountable to the highest standards of use

Users, systems and (where appropriate) devices are identified and authenticated prior to being permitted access to information or systems

All staff have been notified that their system use could be monitored

### Control Objective

The organisation obtains documented evidence that Systems Administrators have been made aware of their increased responsibilities with respect to acceptable use.

### Approach

1. Determine if the organisation requires System Administrators to sign a document that outlines their increased responsibilities with respect to acceptable use. These responsibilities could include not using their administrator account for tasks that do not require elevated access.

2. For a sample of the organisation's System Administrators, review evidence that they have signed this enhanced acceptable use policy statement.

### Assessment Documentation

1. Signed copy of agreements signed by system administrators.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 4: Assertion 3

## Evidence Item 4.3.2

All staff understand that their activities on IT systems will be monitored and recorded for security purposes.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All system administrators have signed an agreement which holds them accountable to the highest standards of use

Users, systems and (where appropriate) devices are identified and authenticated prior to being permitted access to information or systems

All staff have been notified that their system use could be monitored

### Control Objective

The organisation has processes and technologies in place to enable users, systems and devices to be identified and authenticated prior to being provided access to information or systems.

### Approach

1. Determine if the organisation has an overarching strategy/policy/procedure for authentication, ensuring that the strength of authentication mechanisms are proportionate to the criticality of the systems/information they protect.

2. For a sample of the organisation's systems containing personal data or devices affording access to personal data; review the authentication requirements/settings and confirm that they are in line with the organisation's strategy/policy. In addition, confirm that they enable the authentication of users, devices and systems prior to granting access to the information or systems. Alternatively, look at a sample of the access requests to see whether access has been appropriately granted on the system.

### Assessment Documentation

1. Authentication strategy/policy/process.

2. Access control policy/process.

# Standard 4: Assertion 3

## Evidence Item 4.3.3

All staff understand that their activities on IT systems will be monitored and recorded for security purposes.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All system administrators have signed an agreement which holds them accountable to the highest standards of use

Users, systems and (where appropriate) devices are identified and authenticated prior to being permitted access to information or systems

All staff have been notified that their system use could be monitored

### Control Objective

In order to align with data protection regulations, staff are informed that their IT system use could be monitored.

### Approach

1. Determine if staff are informed that their IT system use could be monitored. Review evidence associated with them being informed, and confirm that they are re-informed on at least an annual basis.

### Assessment Documentation

1. Evidence that staff are informed that their IT system use could be monitored on at least an annual basis.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 4: Assertion 4

You closely manage privileged user access to networks and information systems supporting the essential service.

## Objective

Privileged users typically have access to large volumes of an organisation's confidential data, as well as being able to make administrator level changes to its infrastructure and systems. Threat actors target these accounts, making it essential that organisations manage privileged user access effectively.

**Category 2**

# Standard 4: Assertion 4

## Evidence Item 4.4.1

You closely manage privileged user access to networks and information systems supporting the essential service.

**Mandatory**

| Category |
| --- |
| 2 |

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

**The organisation ensures that logs, including privileged account use, are kept securely and only accessible to appropriate personnel. They are stored in a read only format, tamper proof and managed according to the organisation information life cycle policy with disposal as appropriate.**

The organisation does not allow users with wide ranging or extensive system privilege to use their highly privileged accounts for high-risk functions, in particular email and web browsing.

The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation.

### Control Objective

The organisation has documented a log retention policy that outlines its approach to storing the logs of authenticated users. This policy should include details on maintaining the integrity of the logs, offline backup for disaster recovery purposes, internet logs and mobile device/tablet logs.

### Approach

1. Discuss with Management to determine whether the organisation has documented a log retention policy. If in place, review the log management policy to determine whether the sections outlined in the control objective column are included.

2. Determine whether, in line with the log retention policy, logs are retained for a minimum of six months to enable their use for the detection of potential malicious activity.

3. Enquire with Management as to the processes, automated or manual, for reviewing logs to proactively or retrospectively identify any potential incidents.

4. Depending on the response to 2, review evidence associated with the control implementation. For example, if a Security Incident and Events Monitoring (SIEM) solution has been implemented to automatically review logs, reporting from the SIEM could be reviewed. If a manual log review process is in place, any associated evidence could be reviewed.

### Assessment Documentation

1. Log retention policy.
2. Documentation associated with automated or manual log review controls.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 4: Assertion 4

## Evidence Item 4.4.2

You closely manage privileged user access to networks and information systems supporting the essential service.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

The organisation ensures that logs, including privileged account use, are kept securely and only accessible to appropriate personnel. They are stored in a read only format, tamper proof and managed according to the organisation information life cycle policy with disposal as appropriate.

**The organisation does not allow users with wide ranging or extensive system privilege to use their highly privileged accounts for high-risk functions, in particular email and web browsing.**

The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation.

### Control Objective

Users with elevated levels of access do not use their privileged accounts for performing high risk functions, such as reading emails or browsing the internet.

### Approach

1. Determine if the organisation has prohibited privileged users, via policy, from using their privileged accounts for high risk activities that do not require elevated access, such as reading emails or browsing the internet. This could be enforced through Active Directory or local Group Policies. If applicable, review the organisation's Group Policy configurations.

2. For a sample of system administrators, confirm that they have a normal user account, as well as their administrator account. Request to be shown evidence that such users switch to use of their normal account for tasks and activities when administration privileges are not required.

3. Review the mechanisms that the organisation has in place to raise awareness of this policy with privileged users.

### Assessment Documentation

1. Access management policy including a control that prohibits privileged users from using their privileged accounts for high risk activities that do not require elevated access, such as reading emails or browsing the internet.

# Standard 4: Assertion 4

## Evidence Item 4.4.3

You closely manage privileged user access to networks and information systems supporting the essential service.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

The organisation ensures that logs, including privileged account use, are kept securely and only accessible to appropriate personnel. They are stored in a read only format, tamper proof and managed according to the organisation information life cycle policy with disposal as appropriate.

The organisation does not allow users with wide ranging or extensive system privilege to use their highly privileged accounts for high-risk functions, in particular email and web browsing.

**The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation.**

### Control Objective

Privileged access is only granted on devices that are owned and managed by the organisation. Exceptions to this policy are formally approved and recorded. This reduces the risk of an attacker obtaining privileged access to the organisation's network, systems and data by exploiting vulnerabilities on an unmanaged device.

### Approach

1. Understand if the organisation has a documented policy that prevents Privileged user access rights being granted on a non-corporate device.

2. Review how effectively this control has been designed and implemented, for example, if there is a requirement to review the device that the account will be accessed through as part of the account provisioning process.

3. Determine if there are any exceptions to this policy, and how any exceptions are formally approved and managed. Mitigating controls, such as increased monitoring of the Privileged user accounts, could be implemented.

4. Determine if the organisation has implemented a Network Access Control (NAC) solution to control which assets can access the network, and to what extent. If a NAC solution is already in place, ensure that the policies are appropriate and are being enforced. If a NAC solution isn't in place; ask the accountable person what mitigating controls or alternatives help achieve the same security outcome.

Continued

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 4: Assertion 4

## Evidence Item 4.4.3

You closely manage privileged user access to networks and information systems supporting the essential service.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

The organisation ensures that logs, including privileged account use, are kept securely and only accessible to appropriate personnel. They are stored in a read only format, tamper proof and managed according to the organisation information life cycle policy with disposal as appropriate.

The organisation does not allow users with wide ranging or extensive system privilege to use their highly privileged accounts for high-risk functions, in particular email and web browsing.

**The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation.**

### Assessment Documentation

1. Access/Privileged access management policy including a control that Privileged accounts can only be accessed via corporate devices.

2. Privileged access account provisioning process including a review of the device that will be used to access the Privileged account.

3. Policy exceptions and associated approvals.

4. NAC solution configurations, or details of other mitigating controls.

Previous

Back

# Standard 4: Assertion 5

You ensure your passwords are suitable for the information you are protecting

## Why does this matter?

In order to secure access to an organisation's infrastructure, applications and data, a password policy should be implemented that is in line with industry good practice. Other technical controls should also be implemented to protect against brute force attacks and password guessing, such as account lockout after a number of unsuccessful authentication attempts.

**Category 2**

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 4: Assertion 5

## Evidence Item 4.5.1

You ensure your passwords are suitable for the information you are protecting.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation has a password policy giving staff advice on managing their passwords

Technical controls enforce password policy and mitigate against password-guessing attacks.

Multi-factor authentication is enforced on all remote access and privileged user accounts on all systems, with exceptions only as permitted by the national MFA policy.

Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.

Your organisation, or your supply chain with access to your systems, grant limited privileged access and third party access only for a limited time period, or is planning to do so.

### Control Objective

A password policy is documented that outlines the security requirements for passwords used across the organisation.

### Approach

1. Determine if a password policy has been formally documented and reviewed within its review cycle.

2. Review the password policy and confirm that the following are included:

(a) How to avoid choosing obvious passwords (such as those based on easily-discoverable information);

(b) Not to choose common passwords (use of technical means, using a password blocklistrecommended);

(c) No password reuse;

(d) Where and how they may record passwords to store and retrieve them securely;

(e) If password management software is allowed, if so, which; and

(f) Which passwords they really must memorise and not record anywhere.

### Assessment Documentation

1. Password policy.

Back

# Standard 4: Assertion 5

## Evidence Item 4.5.2

You ensure your passwords are suitable for the information you are protecting.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation has a password policy giving staff advice on managing their passwords

**Technical controls enforce password policy and mitigate against password-guessing attacks.**

Multi-factor authentication is enforced on all remote access and privileged user accounts on all systems, with exceptions only as permitted by the national MFA policy.

Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.

Your organisation, or your supply chain with access to your systems, grant limited privileged access and third party access only for a limited time period, or is planning to do so.

### Control Objective

Attackers use a variety of techniques to discover passwords, for example password spraying (using a small number of commonly-used passwords in an attempt to access a large number of accounts) and brute-force attacks (the automated guessing of large numbers of passwords until the correct one is found).

A system's security should therefore always rely on effective technical controls, particularly with regards to enforcing password policy and mitigating against password-guessing attacks.

### Approach

1. Determine if the policy requires configuration of password controls such that there is a time delay between successive login attempts- a technique known as 'throttling'. This restricts the number of guesses an attacker can attempt while giving users multiple opportunities to remember their password. Alternatively (or as well as throttling), determine if the organisation is applying account lockout controls, where a user only has a fixed number of attempts to answer their password before their account is locked.

2. Determine if the policy requires security monitoring to detect and alert the organisation to what may be indicators of malicious or abnormal behaviours, such as: login attempts that fail the second step of Multi Factor Authentication and brute-forcing of account passwords, including password spraying.

Continued

Back

# Standard 4: Assertion 5

## Evidence Item 4.5.2

You ensure your passwords are suitable for the information you are protecting.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation has a password policy giving staff advice on managing their passwords

Technical controls enforce password policy and mitigate against password-guessing attacks.

Multi-factor authentication is enforced on all remote access and privileged user accounts on all systems, with exceptions only as permitted by the national MFA policy.

Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.

Your organisation, or your supply chain with access to your systems, grant limited privileged access and third party access only for a limited time period, or is planning to do so.

### Approach (continued)

3. Determine if the policy requires the use of a password deny list that prevents the most common (and therefore easily guessed) passwords being used. If an organisation can't deny list passwords at the point they are created, it might be possible to reactively search a password database for the hashes of deny list passwords. If the organisations does this and a high number of common passwords are found, determine if the organisation offers training to users regarding their management and choosing of passwords.

*N.B.* Throttling is normally preferred to account lockout, because account lockout can leave legitimate users unable to access their accounts, and requires access to an account recovery method. In addition, account lockout can provide an attacker with an easy way to launch a denial of service attack, particularly for large online systems. Also, if using account lockout, it is often recommended that the control allows between 5 and 10 login attempts before the account is frozen, to avoid accidental lockout. Through discussion, understand the thought process or risk assessment process the organisation went through to decide on technical controls to enforce the password policy.

Previous

Continued

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 4: Assertion 5

## Evidence Item 4.5.2

You ensure your passwords are suitable for the information you are protecting.

Mandatory

| Category |
| --- |
| 2 |

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation has a password policy giving staff advice on managing their passwords

**Technical controls enforce password policy and mitigate against password-guessing attacks.**

Multi-factor authentication is enforced on all remote access and privileged user accounts on all systems, with exceptions only as permitted by the national MFA policy.

Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.

Your organisation, or your supply chain with access to your systems, grant limited privileged access and third party access only for a limited time period, or is planning to do so.

### Assessment Documentation

1. Password policy- rules regarding time delay between successive login attempts and/or account lockout.
2. Network password settings.
3. Application password settings.
4. Security Monitoring reports focused on detecting and alerting indicators of malicious or abnormal behaviour, for example:
   - login attempts that fail the second step of MFA;
   - brute-forcing of account passwords, including password spraying;
   - Login attempts from unexpected geographic areas; and
   - Reports of unexpected account lockouts or other unusual account behaviour from users.
5. Password deny lists.

Previous

# Standard 4: Assertion 5

## Evidence Item 4.5.3

You ensure your passwords are suitable for the information you are protecting.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation has a password policy giving staff advice on managing their passwords

Technical controls enforce password policy and mitigate against password-guessing attacks.

**Multi-factor authentication is enforced on all remote access and privileged user accounts on all systems, with exceptions only as permitted by the national MFA policy.**

Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.

Your organisation, or your supply chain with access to your systems, grant limited privileged access and third party access only for a limited time period, or is planning to do so.

### Control Objective

Multi-factor authentication (e.g. two or more of 'something you know', 'something you have' and 'something you are') has been implemented where appropriate and technically feasible.

### Approach

**For Independent Providers**

1. Discuss the organisation's approach to authentication with the appropriate individual and determine the Multi Factor Authentication approach.

2. Review the approach has been documented in an authentication strategy/plan,

review it to assess the extent to which Multi Factor Authentication has been considered in line with the national MFA policy.

**For IT Suppliers**

1. Discuss the organisation's approach to authentication with the appropriate individual and determine the Multi Factor Authentication approach.

2. Assess whether there is a process by which information systems which allow remote access and privileged user accounts, that do not have Multi Factor Authentication, are escalated to senior management for review and potential exception.

3. Review a sample of exceptions and determine for each whether the risk associated with not applying multi factor authentication is properly documented, assessed and accepted by the organisation's Board or senior management.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 4: Assertion 5

## Evidence Item 4.5.3

You ensure your passwords are suitable for the information you are protecting.

**Mandatory**

| Category |
| --- |
| 2 |

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation has a password policy giving staff advice on managing their passwords

Technical controls enforce password policy and mitigate against password-guessing attacks.

**Multi-factor authentication is enforced on all remote access and privileged user accounts on all systems, with exceptions only as permitted by the national MFA policy.**

Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.

Your organisation, or your supply chain with access to your systems, grant limited privileged access and third party access only for a limited time period, or is planning to do so.

### Control Objective

Multi-factor authentication (e.g. two or more of 'something you know', 'something you have' and 'something you are') has been implemented where appropriate and technically feasible.

### Assessment Documentation

**For Independent providers**

1. Authentication strategy/plan.

2. The national MFA policy

**For IT Suppliers**

1. Authentication strategy/plan.

2. Sample of Multi factor authentication exceptions

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 4: Assertion 5

## Evidence Item 4.5.4

You ensure your passwords are suitable for the information you are protecting.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation has a password policy giving staff advice on managing their passwords

Technical controls enforce password policy and mitigate against password-guessing attacks.

Multi-factor authentication is enforced on all remote access and privileged user accounts on all systems, with exceptions only as permitted by the national MFA policy.

**Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.**

Your organisation, or your supply chain with access to your systems, grant limited privileged access and third party access only for a limited time period, or is planning to do so.

### Control Objective

To prevent their exploitation by an attacker, passwords for; system accounts, social media accounts and infrastructure components are changed from their default values and replaced with secure passwords in line with the organisation's password policy.

### Approach

1. Through discussion with Management, determine how the organisation ensures that default passwords are changed as part of the implementation of a system or infrastructure component.

2. Review relevant system/infrastructure implementation procedures to determine if there is an action to change all passwords from their default values.

3. Determine if the organisation's password policy includes social media accounts in scope, and has appropriate password complexity requirements.

### Assessment Documentation

1. System/infrastructure implementation procedure.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 4: Assertion 5

## Evidence Item 4.5.5

You ensure your passwords are suitable for the information you are protecting.

| Category |
| --- |
| 2 |

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation has a password policy giving staff advice on managing their passwords

Technical controls enforce password policy and mitigate against password-guessing attacks.

Multi-factor authentication is enforced on all remote access and privileged user accounts on all systems, with exceptions only as permitted by the national MFA policy.

Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.

**Your organisation, or your supply chain with access to your systems, grant limited privileged access and third party access only for a limited time period, or is planning to do so.**

### Control Objective

Privileged and third party access to the organisation's infrastructure must be pre-approved, is time limited to the length of time required to carry out the activity, which is monitored and subjected to logging.

### Approach

1. Identify if the organisation has a standardised process for granting third party and Privileged access to its IT infrastructure.

2. Review if this process contains requirements for both the access being approved by an appropriate individual in the organisation, and the access being time limited.

3. Assess if there is a technical solution in place to minimise the access to the length of time required to carry out the activity.

### Assessment Documentation

1. Privileged access management policy/procedure.

2. Third party/supplier access policy/procedure.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 5 - Process Reviews

The NHS Big Picture Guidance

Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security. Past security breaches and near misses are recorded and used to inform periodic workshops to identify and manage problem processes. User representation is crucial. This should be a candid look at where high risk behaviours are most commonly seen, followed by actions to address these issues while not making life more painful for users (as pain will often be the root cause of an insecure workaround). If security feels like a hassle, it's not being done properly.

**Typical departments responsible for this standard:** Operations, IT Operations, IT Security Operations and Data Security and Protection

## Overview of standard

### Assertion 1

Process reviews are held at least once per year where data security is put at risk following data security incidents.

### Assertion 2

Action is taken to address problem processes as a result of feedback at meetings or in year.

Back

# Standard 5: Assertion 1

Process reviews are held at least once per year where data security is put at risk and following data security incidents.

## Objective

Continuously re-evaluating the security risk associated with an organisation's operational processes is a key step in identifying actions to improve an organisation's data security and protection control environment. It is particularly important to do so after a security incident or 'near miss'.

**Category 2**

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 5: Assertion 1

## Evidence Item 5.1.1

Process reviews are held at least once per year where data security is put at risk and following data security incidents.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security or protection incident, with findings acted upon.

### Control Objective

The organisation identifies the root cause of data security and protection incidents, in order to design and implement mitigating controls to either prevent similar incidents from occurring in the future or to be in a position to better manage them if they do occur.

### Approach

1. Review the organisation's data security and protection incident management procedure. Confirm that it includes a mechanism for identifying the root cause of an incident as part of the lessons learned exercise.

2. Select a sample of data security and protection incidents and confirm that the root cause of the incident has been identified. Review the nature of each of the sampled incidents and confirm that the root cause appears to be appropriate, and has associated mitigating actions assigned with ownership and implementation dates.

3. For the incidents sampled, confirm that controls have been implemented/enhanced, or other steps have been taken, to prevent similar incidents from occurring in the future.

### Assessment Documentation

1. Data security and protection incident management procedure.

2. Documentation associated with a sample of incidents with details on the root cause of the incident.

3. Evidence associated with action being taken to prevent similar incidents from occurring in the future.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 5: Assertion 2

Action is taken to address problem processes as a result of feedback at meetings or in year.

## Objective

In order to be effective, problem processes are being monitored and controlled. Problem processes are processes which are repeatedly linked to incidents or near misses. Processes can also be categorised as problem processes if they are linked to one high profile (or high value) incident or near miss. in question. All relevant stakeholders including security practitioners should be included to help identify and suggest improvements to the process in order to reduce any associated security risks.

**Category 2**

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 5: Assertion 2

## Evidence Item 5.2.1

Action is taken to address problem processes as a result of feedback at meetings or in year.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Actions to address problem processes are being monitored, and assurance is given to the board or equivalent senior team.

### Control Objective

The organisation effectively manages and reports on its security and data protection improvements to its senior leadership team.

### Approach

1. Assess how the organisation manages and reports on operational process improvements, including if outstanding actions are escalated to its senior leadership team. Request and review a sample of any such reports, as well as a sample of minutes from the organisation's Board (or equivalent) that these are reported to. Review the minutes and confirm that the reports are discussed, and any outstanding actions highlighted.

2. Select a sample of actions generated from the previous years' process review, and confirm that they have been implemented.

### Assessment Documentation

1. Security improvements tracker.

2. Security improvements report.

3. Board (or equivalent) minutes.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 6 - Responding to Incidents

The NHS Big Picture Guidance

Cyberattacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken as soon as possible following a data breach or near miss, with a report made to senior management within 12 hours of detection. Significant cyberattacks are to be reported to CareCERT immediately following detection.

**Typical departments responsible for this standard:** Information Governance, Legal, Data Security and Protection, IT Security, Security Monitoring/SOC

## Overview of standard

### Assertion 1

A confidential system for reporting data security and protection breaches and near misses is in place and actively used.

### Assertion 2

All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.

### Assertion 3

Known vulnerabilities are acted on based on advice from NHS England, and lessons are learned from previous incidents and near misses

Back

# Standard 6: Assertion 1

A confidential system for reporting data security and protection breaches and near misses is in place and actively used.

## Objective

In order to comply with data protection regulations, and to facilitate internal data security and protection incident management processes, organisations should have a mechanism for reporting and managing security incidents. This should include; how they are reported by staff, recorded centrally, and escalated to a senior level of the organisation for action.

**Category 2**

# Standard 6: Assertion 1

## Evidence Item 6.1.1

A confidential system for reporting data security and protection breaches and near misses is in place and actively used

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

A policy/procedure is in place to ensure data security and protection incidents are managed/reported appropriately.

The board or equivalent have been informed of the action plan for all data security and protection breaches reported to the ICO and/or the DHSC in the last twelve months.

Individuals affected by a breach where there is high risk to their rights and freedoms are appropriately informed.

### Control Objective

The organisation has in place a process/system for reporting resilience, network security, data security and/or personal data breaches or near misses in line with its legal, NIS Directive and DSP Toolkit reporting requirements.

### Approach

1. Request to review a documented procedure (or similar evidence) that outlines the process the organisation has in place for reporting data security and/or personal data breaches and near misses through the DSPT Incident Reporting Tool.

The process should include how the organisation will:

a) Grade the incident according to the significance of the breach and the likelihood of those consequences occurring. This should be aligned to guidance available through the DSPT Incident Reporting Tool.

b) Report the incident within 72 hours of becoming aware of it.

c) Provide the required information in line with the requirements of the GDPR and NIS Directive for reporting personal data breaches or operational resilience breaches. Please refer to the Data Security and Protection (DSP) Toolkit Independent Assessment Guide.

d) Outline who is responsible within the organisation for reporting an incident and ensure the incident is reviewed by either the DPO/Caldicott Guardian or SIRO.

2. Request to review any documented evidence that demonstrates how the organisation has communicated any reporting requirements to its data processors.

Continued

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 6: Assertion 1

## Evidence Item 6.1.1

A confidential system for reporting data security and protection breaches and near misses is in place and actively used

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

A policy/procedure is in place to ensure data security and protection incidents are managed/reported appropriately.

The board or equivalent have been informed of the action plan for all data security and protection breaches reported to the ICO and/or the DHSC in the last twelve months.

Individuals affected by a breach where there is high risk to their rights and freedoms are appropriately informed.

3. Review any evidence to demonstrate that staff are trained in the requirements of incident reporting.

4. Review any evidence that demonstrates any formal testing undertaken by the organisation to provide assurance that the process is being followed in practice.

### Assessment Documentation

1. Procedure (or similar) document outlining the process for reporting incidents through the DSP Toolkit Incident Reporting Tool.

2 Any documented evidence that demonstrates how the organisation has communicated any reporting requirements to its data processors. For example, contract provisions, Data Processing Agreements or any procedures or processes to ensure processors are aware of their obligations to report any incidents to the organisation.

3. Any evidence to demonstrate that staff are trained in the requirements of incident reporting.

4. Any evidence that demonstrates any formal testing undertaken by the organisation to provide assurance that the process is being followed in practice.

Previous

# Standard 6: Assertion 1

## Evidence Item 6.1.2

A confidential system for reporting data security and protection breaches and near misses is in place and actively used

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

A policy/procedure is in place to ensure data security and protection incidents are managed/reported appropriately.

The board or equivalent have been informed of the action plan for all data security and protection breaches reported to the ICO and/or the DHSC in the last twelve months.

Individuals affected by a breach where there is high risk to their rights and freedoms are appropriately informed.

### Control Objective

The organisation has a process in place to provide the Board/individual with overall responsibility for data security/protection with oversight of an action plan for all data security and personal data breaches.

### Approach

1. Request to review a copy of an action plan that outlines clear steps for mitigating risk and/or service improvements required following all incidents recorded.

2. Cross check the action plan against the record of incidents recorded to ensure that there is either an action plan in place for all incidents or, there is a documented reason for an action plan not being required. Does the action plan contain a clear line of responsibility and timescale for completing the work?

3. Review any evidence that demonstrates the action plan is shared:

a) with the Board on at least an annual basis (*Category 1 and 2 organisations*).

b) with the individual responsible for data security/protection on at least an annual basis *(Category 3 and 4 organisations).*

4. Review any evidence that demonstrates how the organisation escalates and manages any actions not completed within the required timescales.

5. Review any evidence that demonstrates how the organisation tests/checks that the action has been completed and is being implemented in practice.

Continued

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 6: Assertion 1

## Evidence Item 6.1.2

A confidential system for reporting data security and protection breaches and near misses is in place and actively used

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

A policy/procedure is in place to ensure data security and protection incidents are managed/reported appropriately.

**The board or equivalent have been informed of the action plan for all data security and protection breaches reported to the ICO and/or the DHSC in the last twelve months.**

Individuals affected by a breach where there is high risk to their rights and freedoms are appropriately informed.

### Assessment Documentation

1. Copy of an action plan in place for all incidents or, a documented reason for an action plan not being required.
2. Record of incidents recorded over the past 12 months.
3. Review any evidence that demonstrates the action plan is shared with the Board or the individual responsible for data security/protection.
4. Evidence that demonstrates how the organisation escalates and manages any actions not completed within the required timescales.
5. Evidence that demonstrates how the organisation tests that the action has been completed and is being implemented in practice.

Previous

# Standard 6: Assertion 1

## Evidence Item 6.1.3

A confidential system for reporting data security and protection breaches and near misses is in place and actively used

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

A policy/procedure is in place to ensure data security and protection incidents are managed/reported appropriately.

The board or equivalent have been informed of the action plan for all data security and protection breaches reported to the ICO and/or the DHSC in the last twelve months.

Individuals affected by a breach where there is high risk to their rights and freedoms are appropriately informed.

### Control Objective

The organisation has a process in place to ensure that individuals affected by an incident are informed where it is likely to result in a high risk in relation to their rights and freedoms.

### Approach

1. Request to review a documented procedure (or similar evidence) that outlines the process the organisation has in place for communicating data security and/or personal data breaches to individuals where the incident is likely to result in a high risk their rights and freedoms.

The process should incorporate how the organisation will:

a) Document the decision process as to whether it will inform individuals of an incident.

b) Report the incident without undue delay.

c) Provide the required information in line with the requirements of the GDPR for communicating personal data breaches to individuals. Please refer to the Data Security and Protection (DSP) Toolkit Independent Assessment Guide.

d) Outline who is responsible within the organisation for leading on the communication of the incident to individuals.

2. Review any evidence to demonstrate that staff are trained in the requirements of communicating an incident.

Continued

# Standard 6: Assertion 1

## Evidence Item 6.1.3

A confidential system for reporting data security and protection breaches and near misses is in place and actively used

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

A policy/procedure is in place to ensure data security and protection incidents are managed/reported appropriately.

The board or equivalent have been informed of the action plan for all data security and protection breaches reported to the ICO and/or the DHSC in the last twelve months.

Individuals affected by a breach where there is high risk to their rights and freedoms are appropriately informed.

3. Select a sample of data security and protection incidents and review communications that were sent to the individuals/data subjects affected by the incident.

### Assessment Documentation

1. Procedure (or similar) document outlining the process for communicating incidents to individuals affected.

2. Any evidence to demonstrate that staff are trained in the requirements of communicating incidents.

3. Any evidence that demonstrates any formal testing undertaken by the organisation to provide assurance that the process is being followed in practice.

4. Communications to individuals/data subjects affected by a sample of data security and protection incidents.

Previous

Back

# Standard 6: Assertion 2

All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.

## Objective

Malware, including ransomware such as WannaCry, are an ever increasing risk to health and social care organisations. This assertion outlines a number of technical controls that could be implemented to protect an organisation against malware. These include; deploying antivirus on endpoints and at the network level, implementing a web filtering solution, and application allow listing/blocklisting.

**Category 2**

# Standard 6: Assertion 2

## Evidence Item 6.2.1

Mandatory

All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

- Antivirus/anti-malware software has been installed on all computers that are connected to, or are capable of connecting to the Internet.
- Antivirus/anti-malware is kept continually up to date.
- Antivirus/anti-malware software scans files automatically upon access.
- Connections to malicious websites on the Internet are prevented.
- Number of phishing emails reported by staff per month.
- You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your organisation's domains to make email spoofing difficult.

6.2 continued

### Control Objective

All servers / workstations / devices / endpoints with an internet connection or capability to access the internet have antivirus installed. Downloading malware via links on malicious emails or websites is the primary mechanism by which machines are infected with malware.

### Approach

1. Understand how the organisation measures the completeness and suitability of the coverage of antivirus across its IT estate, and ensures that antivirus is installed on all devices / computers that may connect to the internet (and review asset management arrangements to assess the confidence that the organisation has a handle on its assets and operates an 'environment of certainty').

2. Review any reporting on the completeness / coverage of antivirus across the organisation's IT estate and determine if there are any instances of workstations / computers being connected to the internet without having antivirus installed. Request and review evidence of the previous three reports on internet connectivity, asset management and/or anti-malware / AV coverage.

3. Review the computer / workstation provisioning process and determine if the installation of antivirus is included, or if antivirus is included in the organisation's standard workshop build.

### Assessment Documentation

1. Previous three reports on the coverage of antivirus across the organisation's IT estate.

2. Workstation provisioning process.

Back

# Standard 6: Assertion 2

## Evidence Item 6.2.3

All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Antivirus/anti-malware software has been installed on all computers that are connected to, or are capable of connecting to the Internet.

**Antivirus/anti-malware is kept continually up to date.**

Antivirus/anti-malware software scans files automatically upon access.

Connections to malicious websites on the Internet are prevented.

Number of phishing emails reported by staff per month.

You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your organisation's domains to make email spoofing difficult.

6.2 continued

### Control Objective

Antivirus signatures are updated on a regular basis to ensure that the organisation's IT infrastructure is protected against new instances of malware.

### Approach

1. Through discussion with Management and/or review of antivirus policies/procedures, determine how often antivirus signatures/rulesets/Indicators of Compromise (IoC) are updated.

2. Review antivirus configurations and assess whether signatures/rulesets are configured to be updated in line with antivirus policies/procedures.

### Assessment Documentation

1. Antivirus policy/procedure.

2. Antivirus configurations.

# Standard 6: Assertion 2

## Evidence Item 6.2.4

All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Antivirus/anti-malware software has been installed on all computers that are connected to, or are capable of connecting to the Internet.

Antivirus/anti-malware is kept continually up to date.

**Antivirus/anti-malware software scans files automatically upon access.**

Connections to malicious websites on the Internet are prevented.

Number of phishing emails reported by staff per month.

You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your organisation's domains to make email spoofing difficult.

6.2 continued

### Control Objective

The organisation's antivirus solution is designed to automatically scan files for malicious content prior to being downloaded.

### Approach

1. Through discussion with Management and/or review of antivirus policies/procedures, determine if the solution is configured to automatically scan files for malicious content prior to being downloaded. Is there a sandbox / safe detonation / payload investigation environment?

2. Review antivirus configurations and assess whether the solution is configured to automatically scan files for malicious content prior to being downloaded.

### Assessment Documentation

1. Antivirus policy/procedure.

2. Antivirus configurations.

3. List of client PCs and Servers

4. Logs of updates made to AV software/virus signatures on servers/appliances

# Standard 6: Assertion 2

## Evidence Item 6.2.5

All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Antivirus/anti-malware software has been installed on all computers that are connected to, or are capable of connecting to the Internet.

Antivirus/anti-malware is kept continually up to date.

Antivirus/anti-malware software scans files automatically upon access.

**Connections to malicious websites on the Internet are prevented.**

Number of phishing emails reported by staff per month.

You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your organisation's domains to make email spoofing difficult.

6.2 continued

### Control Objective

The organisation has implemented technical controls to prevent workstations / computers / devices making connections to malicious websites. This could include deploying a web proxy at the organisation's perimeter.

### Approach

1. Through discussion with Management and/or review of policies/procedures, determine if the organisation has implemented technical controls to prevent external connections to malicious websites.

2. Review evidence of the control implementation (if applicable). This could include receiving alerts from the web proxy when a potentially malicious connection is blocked.

### Assessment Documentation

1. Technical documentation associated with the organisation's controls to prevent external connections to malicious websites.

2. Evidence of implementation of technical controls, for example, web proxy alerts.

# Standard 6: Assertion 2

## Evidence Item 6.2.6

All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Antivirus/anti-malware software has been installed on all computers that are connected to, or are capable of connecting to the Internet.

Antivirus/anti-malware is kept continually up to date.

Antivirus/anti-malware software scans files automatically upon access.

Connections to malicious websites on the Internet are prevented.

**Number of phishing emails reported by staff per month.**

You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your organisation's domains to make email spoofing difficult.

6.2 continued

### Control Objective

There is a process for staff to escalate potentially malicious phishing emails to the relevant team (IT/IT security). Staff (and temps/contractors) are made aware of this process through information security training or another mechanism.

### Approach

This evidence item should only be tested if the organisation has an email exchange / email solution other than NHSmail.

1. Determine if there is a process by which staff can report potentially malicious phishing emails to the relevant department.

2. Review this document and understand how effectively this process has been designed, including if there are multiple reporting mechanisms that could be used in the event of system unavailability for example.

3. Through discussion with Management, understand how staff have been made aware of this process, including through formal information security training or awareness campaigns.

### Assessment Documentation

1. Information security incident reporting procedure.

2. Training and/or awareness material associated with reporting phishing emails.

# Standard 6: Assertion 2

## Evidence Item 6.2.8

All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.

**Mandatory**

| Category |
| --- |
| 2 |

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Antivirus/anti-malware software has been installed on all computers that are connected to, or are capable of connecting to the Internet.

Antivirus/anti-malware is kept continually up to date.

Antivirus/anti-malware software scans files automatically upon access.

Connections to malicious websites on the Internet are prevented.

Number of phishing emails reported by staff per month.

**You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your organisation's domains to make email spoofing difficult.**

6.2 continued

### Control Objective

The organisation has enabled DMARC (Domain-based Messaging, Authentication, Reporting and Conformance), which builds on the authentication standards Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) to prevent its domain being spoofed.

### Approach

This evidence item should only be tested if the organisation has an email exchange / email solution other than NHSmail.

1. Through discussion with Management, understand if DMARC, DKIM and SPF have been implemented on the organisation's domains.

2. Review evidence associated with these standards being implemented. This could include regular DMARC reports. If these reports are received, request and review the previous three reports.

### Assessment Documentation

1. Evidence that DMARC, DKIM and SPF have been implemented on the organisation's domains. This could include regular DMARC reports. If these reports are received, request and review the previous three reports.

# Standard 6: Assertion 2

## Evidence Item 6.2.9

All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

You have implemented spam and malware filtering, and enforce DMARC on inbound email.

6.2 Previous

### Control Objective

The organisation has implemented an email filtering solution, and enforces DMARC (Domain-based Messaging, Authentication, Reporting and Conformance), to prevent potentially malicious emails (including phishing) from reaching the end users' email account.

### Approach

This evidence item should only be tested if the organisation has an email exchange / email solution other than NHSmail.

1. Through discussion with Management and/or review of policies/procedures, determine if the organisation has implemented technical controls to prevent potentially malicious emails (including phishing) from reaching the end users' email account.

2. Review evidence of the control implementation (if applicable). This could include receiving alerts from the email filtering solution when a potentially malicious email is blocked.

3. Review evidence that DMARC has been implemented on inbound email. This could include regular DMARC reports. If these reports are received, request and review the previous three reports.

Continued

# Standard 6: Assertion 2

## Evidence Item 6.2.9

All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

You have implemented spam and malware filtering, and enforce DMARC on inbound email.

1.3 Previous

### Assessment Documentation

1. Technical documentation associated with the organisation's controls to prevent malicious emails.

2. Evidence of implementation of technical controls, for example, email filtering solution alerts.

3. Evidence that DMARC has been implemented on inbound email. This could include regular DMARC reports. If these reports are received, request and review the previous three reports.

Previous

# Standard 6: Assertion 3

Known vulnerabilities are acted on based on advice from NHS England, and lessons are learned from previous incidents and near misses

## Objective

The objective of this assertion is to assess whether an organisation has the appropriate monitoring capabilities (technology and resource), to both detect and respond to a data security and protection incident. Health and social care organisations should also secure their systems based on advice from the CareCERT service provided by NHS England.

**Category 2**

Back

# Standard 6: Assertion 3

Mandatory

## Evidence Item 6.3.1

Known vulnerabilities are acted on based on advice from NHS England, and lessons are learned from previous incidents and near misses

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

**If you have had a data security incident, was it caused by a known vulnerability?**

The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.

The organisation has a proportionate monitoring solution to detect cyber events on systems and services.

All new digital services that are attractive to cyber criminals (such as for fraud) are implementing transactional monitoring techniques from the outset.

Have you had any repeat data security incidents within the organisation during the past twelve months?

### Control Objective

The organisation has acted on advice from CareCERT to prevent data security incidents and has a procedure for maintaining up to date awareness of known vulnerabilities.

### Approach

1. Pick a sample of the organisation's data security incidents and review the root cause to determine if the incidents were caused by known security vulnerabilities.

2. Review the organisation's procedures for becoming aware of and assessing vulnerabilities in relation to the technology deployed on the estate.

### Assessment Documentation

1. Data security incident reports.

Back

# Standard 6: Assertion 3

Mandatory

## Evidence Item 6.3.2

Known vulnerabilities are acted on based on advice from NHS England, and lessons are learned from previous incidents and near misses

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

If you have had a data security incident, was it caused by a known vulnerability?

The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.

The organisation has a proportionate monitoring solution to detect cyber events on systems and services.

All new digital services that are attractive to cyber criminals (such as for fraud) are implementing transactional monitoring techniques from the outset.

Have you had any repeat data security incidents within the organisation during the past twelve months?

### Control Objective

Remedial actions associated with high severity CareCERT alerts are implemented within 48 hours to prevent the vulnerabilities being exploited, resulting in a data security incident.

### Approach

1. If the organisation has responded that all high severity CareCERT alerts have been responded to within 48 hours, pick 10 high severity alerts and confirm that the organisation has indeed responded to the alert appropriately.

### Assessment Documentation

1. Documentation associated with response to high severity CareCERT alerts.

# Standard 6: Assertion 3

## Evidence Item 6.3.3

Known vulnerabilities are acted on based on advice from NHS England, and lessons are learned from previous incidents and near misses

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

If you have had a data security incident, was it caused by a known vulnerability?

The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.

**The organisation has a proportionate monitoring solution to detect cyber events on systems and services.**

All new digital services that are attractive to cyber criminals (such as for fraud) are implementing transactional monitoring techniques from the outset.

Have you had any repeat data security incidents within the organisation during the past twelve months?

### Control Objective

The organisation has designed and implemented technology solutions and processes to detect cyber security events.

### Approach

1. Through discussion with Management, understand the organisation's current security monitoring control environment. This should consider controls in place at both the network and endpoint level. It should also take a risk-based approach to monitoring, ensuring that the organisation's most critical services and assets are in scope of its monitoring solutions.

2. Review evidence associated with the operation of these controls. For example, alerts/reports generated from a network Intrusion Detection System (IDS). Whilst on-site, observe and walk through the IDS/IPS in operation on-screen with the relevant member of the Data Security and Protection (DSP) team.

3. Understand if gaps in the security monitoring control environment have been documented and mitigations put in place. For example, if the scope of a network monitoring solution does not include all of the organisation's network ingress/egress points, have additional monitoring technologies or processes been implemented?

4. Understand if the organisation has a strategy or plan for how it will develop its security monitoring technology and processes over the subsequent 2-3 years.

5. Review documentation associated with any strategies or plans that are in place.

Continued

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 6: Assertion 3

Mandatory

## Evidence Item 6.3.3

Known vulnerabilities are acted on based on advice from NHS England, and lessons are learned from previous incidents and near misses

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

If you have had a data security incident, was it caused by a known vulnerability?

The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.

**The organisation has a proportionate monitoring solution to detect cyber events on systems and services.**

All new digital services that are attractive to cyber criminals (such as for fraud) are implementing transactional monitoring techniques from the outset.

Have you had any repeat data security incidents within the organisation during the past twelve months?

### Assessment Documentation

1. Network diagram showing security monitoring appliances.
2. Security monitoring process/procedure documentation.
3. Alerts/reports evidencing the current security monitoring control environment.
4. Risk acceptances or other documentation outlining the organisation's security monitoring gaps and mitigating controls that have been put in place.
5. Security monitoring strategy/plan (or similar).

Previous

# Standard 6: Assertion 3

Mandatory

## Evidence Item 6.3.4

Known vulnerabilities are acted on based on advice from NHS England, and lessons are learned from previous incidents and near misses

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

If you have had a data security incident, was it caused by a known vulnerability?

The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.

The organisation has a proportionate monitoring solution to detect cyber events on systems and services.

**All new digital services that are attractive to cyber criminals (such as for fraud) are implementing transactional monitoring techniques from the outset.**

Have you had any repeat data security incidents within the organisation during the past twelve months?

### Control Objective

For new digital services that could be susceptible to fraud, transaction-level monitoring has been implemented to assist in the identification of potential instances of fraudulent activity.

### Approach

1. Determine whether the organisation has assessed which of its digital services are susceptible to fraud, based on the nature of the service and the amount and type of data that it processes.

2. Assess whether there is a requirement that transaction-level monitoring is included in any new digital service that could be susceptible to fraud.

3. If any such services have been implemented during the previous 12 months, review evidence that transaction-level monitoring has been included.

### Assessment Documentation

1. Fraud risk assessment associated with each of the organisation's digital services.

2. System/services requirements documentation that includes transaction-level monitoring in any new digital service that could be susceptible to fraud.

3. Evidence that transaction-level monitoring has been implemented for any such service/application in the previous 12 months.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 6: Assertion 3

## Evidence Item 6.3.5

Known vulnerabilities are acted on based on advice from NHS England, and lessons are learned from previous incidents and near misses

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

If you have had a data security incident, was it caused by a known vulnerability?

The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.

The organisation has a proportionate monitoring solution to detect cyber events on systems and services.

All new digital services that are attractive to cyber criminals (such as for fraud) are implementing transactional monitoring techniques from the outset.

**Have you had any repeat data security incidents within the organisation during the past twelve months?**

### Control Objective

The organisation identifies and reports on the root cause of data security incidents to prevent similar incidents occurring.

### Approach

1. Determine if the organisation's data security incident management procedure includes a requirement to perform 'lessons learned' exercises to identify the root cause of incidents.

2. Understand how the organisation reports on/analyses root causes from data security incidents, and implements mitigations to prevent similar incidents reoccurring.

3. By reviewing the organisation's data security and protection incidents in the previous 12 months, at a high level, determine whether there may be underlying root causes that the organisation has not identified.

### Assessment Documentation

1. Data security incident management procedure.

2. Data security incident root causes reporting.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 7 - Continuity Planning

The NHS Big Picture Guidance

A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management. A business continuity exercise is run every year as a minimum. Those in key roles will receive dedicated training so as to make judicious use of the available materials, ensuring that planning is modelled around the needs of their own business. There should be a clear focus on enabling senior management to make good decisions, and this requires genuine understanding of the topic, as well as the good use of plain English.

**Typical departments responsible for this standard:** Incident Response, Data Security and Protection, Business Continuity, IT Resilience

## Overview of standard

### Assertion 1

Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services.

### Assertion 2

There is an effective test of the continuity plan and disaster recovery plan for data security incidents.

### Assertion 3

You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.

Back

# Standard 7: Assertion 1

Organisations have a defined, planned and communicated response to data security incidents that impact sensitive information or key operational services.

## Objective

In order to design a secure and resilient IT infrastructure, organisations must first understand and document its key operational services and their IT dependencies. The organisation should then develop its resilience and business continuity framework based on this understanding.

**Category 2**

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 7: Assertion 1

Mandatory

## Evidence Item 7.1.1

Organisations have a defined, planned and communicated response to data security incidents that impact sensitive information or key operational services.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

**Your organisation understands the health and care services it provides.**

Your organisation has well defined processes in place to ensure the continuity of services in the event of a data security incident, failure or compromise.

You understand the resources and information that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.

You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.

### Control Objective

The organisation has an understanding of the health and care services it provides, and has documented the key dependencies for each service to continue to be delivered effectively, including technology and physical infrastructure. This helps define and determine the appropriateness of the resilience arrangements for each service and the controls to safeguard confidentiality, integrity and availability of data and information systems on which health and care services rely.

### Approach

1. Request the documentation / evidence where the organisation outlines its operational services along with the key dependencies for each service.

2. Review the document and determine whether it considers

(a) What the organisation's key services are;
(b) What technologies and services their services rely on to remain available and secure;
(c) What other dependencies the operational services have (power, cooling, data, people etc.); and
(d) The impact of loss of availability of the service.

3. Determine how frequently this document is reviewed and updated to incorporate new services. This should be a maximum of 12 months.

Continued

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 7: Assertion 1

Mandatory

## Evidence Item 7.1.1

Organisations have a defined, planned and communicated response to data security incidents that impact sensitive information or key operational services.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation understands the health and care services it provides.

Your organisation has well defined processes in place to ensure the continuity of services in the event of a data security incident, failure or compromise.

You understand the resources and information that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.

You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.

4.From the understanding of the business, pick a sample of key, known services and confirm that they have been included in the dependency mapping.

### Assessment Documentation

1. List of the organisation's key operational services.
2. Mapping/impact analysis of the dependencies that each service relies on.
3. Evidence of the document being reviewed and updated on a regular basis.

Previous

# Standard 7: Assertion 1

Mandatory

## Evidence Item 7.1.2

Organisations have a defined, planned and communicated response to data security incidents that impact sensitive information or key operational services.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation understands the health and care services it provides.

**Your organisation has well defined processes in place to ensure the continuity of services in the event of a data security incident, failure or compromise.**

You understand the resources and information that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.

You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.

### Control Objective

The organisation has Business Continuity arrangements in place, with Business Continuity Plans (BCPs) that outline how the organisation would respond and continue to provide its key services in the event of a data security incident, failure or compromise. BCPs are clear as regards people, resource and information requirements for service continuity purposes.

### Approach

1. Determine if the organisation has defined BCPs that would allow it to continue to provide its key services in the event of a major incident affecting those services. These should include roles and responsibilities, resource and information requirements, as well as clear and concise guidance on the actions to take during the incident. They should also be stored in a physical format so that they could be used in the event of the organisation's systems being unavailable.

2. From the understanding of the business, pick a sample of key, known services and confirm that they have associated BCPs. Also review if the BCPs contain the detail outlined in 1 above.

### Assessment Documentation

1. Business Continuity Policy.

2. Example Business Continuity Plans (BCPs).

# Standard 7: Assertion 1

## Evidence Item 7.1.3

Organisations have a defined, planned and communicated response to data security incidents that impact sensitive information or key operational services.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation understands the health and care services it provides.

Your organisation has well defined processes in place to ensure the continuity of services in the event of a data security incident, failure or compromise.

**You understand the resources and information that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.**

You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.

### Control Objective

The organisation has Business Continuity arrangements in place, with Business Continuity Plans (BCPs) that outline how the organisation would respond and continue to provide its key services in the event of a data security incident, failure or compromise. BCPs are clear as regards people, resource and information requirements for service continuity purposes.

### Approach

1. Determine if the organisation has defined BCPs that would allow it to continue to provide its key services in the event of a data security incident, failure or compromise, including reverting to manual operation. These should include roles and responsibilities, resource and information requirements, as well as clear and concise guidance on the actions to take during the incident. They should also be stored in a physical format so that they could be used in the event of the organisation's systems being unavailable.

2. From the understanding of the business, pick a sample of key, known services and confirm that they have associated BCPs. Also review if the BCPs contain the detailed outlined in 1 above.

### Assessment Documentation

1. Business Continuity Policy.

2. Example Business Continuity Plans (BCPs).

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 7: Assertion 1

## Evidence Item 7.1.4

Organisations have a defined, planned and communicated response to data security incidents that impact sensitive information or key operational services.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation understands the health and care services it provides.

Your organisation has well defined processes in place to ensure the continuity of services in the event of a data security incident, failure or compromise.

You understand the resources and information that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.

**You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.**

### Control Objective

The organisation proactively consumes a variety of relevant threat intelligence sources and has the means to make decisions on actionable intelligence to make appropriate changes to its security control environment to mitigate relevant threats.

### Approach

1. Through discussion with Management, determine the sources of relevant, valuable threat intelligence that the organisation receives.

2. Understand how this threat intelligence is consumed - reviewed, analysed and actioned; and determine if the intelligence is proactively used to mitigate potential threats.

3. For each source of threat intelligence, request the three previous reports/outputs and review any evidence of them being consumed.

### Assessment Documentation

1. Threat intelligence policy/process.

2. Threat intelligence reports/outputs.

3. Evidence of the threat intelligence reports/outputs being consumed.

Back

# Standard 7: Assertion 2

There is an effective test of the continuity plan and disaster recovery plan for data security incidents.

## Objective

After documenting its key operational services and their IT dependencies, organisations should create Business Continuity Plans (BCPs) that outline how a level of service as close to normal service as possible would be maintained in the event of a serious security incident, or other significant event. In order to ensure that they are fit for purpose, these should be tested on a regular basis.

**Category 2**

Back

# Standard 7: Assertion 2

## Evidence Item 7.2.1

There is an effective test of the continuity plan and disaster recovery plan for data security incidents.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Explain how your data security incident response and management plan has been tested to ensure all parties understand their roles and responsibilities as part of the plan.

From the business continuity exercise, explain what issues and actions were documented, with names of actionees listed against each item.

### Control Objective

The organisation tests its data security incident response and management plan on an annual basis to help ensure the preparedness of the organisation to respond, as well as assessing the ongoing appropriateness of the plan itself.

### Approach

1. Through discussion with Management / the accountable person, review how the organisation tests its data security incident response and management plan.

2. Determine whether the appropriate stakeholders e.g. senior (board-level) and members of the operational teams are appropriately briefed, trained and involved in the test.

3. Review collateral associated with the test and determine if actions are recorded during the test and used to continuously improve the plan.

### Assessment Documentation

1. Collateral associated with the most recent test of the data security incident response and management plan.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 7: Assertion 2

## Evidence Item 7.2.2

There is an effective test of the continuity plan and disaster recovery plan for data security incidents.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Explain how your data security incident response and management plan has been tested to ensure all parties understand their roles and responsibilities as part of the plan.

From the business continuity exercise, explain what issues and actions were documented, with names of actionees listed against each item.

### Control Objective

During Business Continuity exercises, issues and actions are recorded and assigned to individuals with defined timescales. This enables the continuous improvement of the plan.

### Approach

1. Review collateral associated with Business Continuity tests conducted over the previous 12 months and confirm that issues and actions are recorded and assigned to individuals. In addition, each action should have a defined timescale to be implemented.

2. Review evidence that the issues and actions recorded were implemented within the defined timescales.

### Assessment Documentation

1. Collateral associated with all BCP tests in the previous 12 months; test plans, test results and recommended remediation actions and improvements.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 7: Assertion 3

You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.

## Objective

The objective of this assertion is to assess whether an organisation has the capability to respond effectively to a data security and protection incident, including; whether it has access to specialist resource, has draft press releases prepared, and is able to backup the data that it needs to run its key services in a timely manner.

**Category 2**

# Standard 7: Assertion 3

## Evidence Item 7.3.1

Mandatory

You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary

All emergency contacts are kept securely, in hardcopy and are up-to-date

Draft press materials for data security incidents are ready

Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed

Your organisation tests its backups regularly to ensure it can restore from a backup.

Your organisation's backups are kept securely and separate from your network ('offline'), or in a cloud service designed for this purpose.

### Control Objective

The organisation has the technical capability to respond to a data security incident. This could include either in-house digital forensic/incident response expertise, or through support from a third party. The organisation is able to leverage support and insight from health and social care bodies such as NHS England, bodies such as NCSC, NCA/NCCU and from insurers and the fourth parties they use, where applicable.

### Approach

1. Review the organisation's data security incident response plan and determine if it includes how technical (in-house or third party) resources would be deployed during an incident. Review documentation concerning forensic readiness, preservation of evidence for investigation, root cause analysis, containment, eradication and prosecution purposes.

2. Where third party resource would be deployed, review the contract/agreement with the third party and assess whether there is a requirement for the third party to respond shortly after the incident being identified (several hours).

3. Where in-house, technical resource would be deployed, review evidence that the individuals receive the appropriate training and have the capability to execute these responsibilities.

Continued

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 7: Assertion 3

Mandatory

## Evidence Item 7.3.1

You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

- On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary
- All emergency contacts are kept securely, in hardcopy and are up-to-date
- Draft press materials for data security incidents are ready
- Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed
- Your organisation tests its backups regularly to ensure it can restore from a backup.
- Your organisation's backups are kept securely and separate from your network ('offline'), or in a cloud service designed for this purpose.

4. For a sample of a single data security and protection incident, review any relevant communications with third parties that supported with the investigation / response to the incident.

### Assessment Documentation

1. Data security incident response plan.
2. Forensic/incident response supplier contract / retainer / insurance policy.
3. Evidence of training/capability of in-house forensic/incident response resource.

Previous

# Standard 7: Assertion 3

Mandatory

## Evidence Item 7.3.2

You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary

All emergency contacts are kept securely, in hardcopy and are up-to-date

Draft press materials for data security incidents are ready

Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed

Your organisation tests its backups regularly to ensure it can restore from a backup.

Your organisation’s backups are kept securely and separate from your network ('offline'), or in a cloud service designed for this purpose.

### Control Objective

The organisation stores its emergency contacts in hard copy for use during a data security incident, where the organisation's systems may be unavailable.

### Approach

1. Review where the organisation stores the hard copy of its emergency contacts and determine if it is accessible to staff with responsibilities for incident response (there should be a copy available off-site if necessary). Review arrangements generally for communication and contact in the event of systems and network unavailability.

### Assessment Documentation

1. Hard copy of emergency contacts.

2. Documentation concerning communication and contact arrangements and procedures in the event of system and network availability issues.

# Standard 7: Assertion 3

## Evidence Item 7.3.3

You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary

All emergency contacts are kept securely, in hardcopy and are up-to-date

**Draft press materials for data security incidents are ready**

Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed

Your organisation tests its backups regularly to ensure it can restore from a backup.

Your organisation's backups are kept securely and separate from your network ('offline'), or in a cloud service designed for this purpose.

### Control Objective

The organisation has drafted and approved, at the Board level, press material that could form part of statements that could be released in the event of a data security incident and the organisation has suitable procedures for agreeing statements and materials in the event of an incident that can't be prepared for pre-emptively.

### Approach

1. Review press statements that the organisation has prepared and approved to be released, when appropriate, in the event of a data security incident.

2. Determine whether these have been approved by an appropriate, Board-level individual.

3. Review the procedure for agreeing material during an incident / in the event of a data security incident.

### Assessment Documentation

1. Approved press statements.

2. Comms / Communications procedures and governance arrangements for agreeing statements at the time / during an incident.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 7: Assertion 3

Mandatory

## Evidence Item 7.3.4

You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary

All emergency contacts are kept securely, in hardcopy and are up-to-date

Draft press materials for data security incidents are ready

**Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed**

Your organisation tests its backups regularly to ensure it can restore from a backup.

Your organisation's backups are kept securely and separate from your network ('offline'), or in a cloud service designed for this purpose.

### Control Objective

The organisation makes backups of all of the data required to effectively recover its key services. These backups are tested on a regular (basis at least annually).

### Approach

1. Determine if the organisation has a backup policy/procedure. Review the policy/procedure and assess if it includes details on how often the organisation backs up its most important data, and how long these backups are stored for. The procedure should also include the steps that would be taken if the organisation has to restore from backups.

2. Determine if Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) have been defined for the organisation's key systems. These should be agreed with the business to ensure that requirements are met. For at least 3 (suitable number to be determined by the auditor, based on the organisation type and size) of the organisation's key systems, review the relevant RTOs and RPOs, along with evidence that these have been agreed with the business.

3. Determine if tests of the backups are performed on a regular basis to assess their ability to meet the defined RTOs and RPOs. For a sample of the organisation's key systems, review evidence that these have been completed.

### Assessment Documentation

1. Backup policy/procedure.

2. RTOs and RPOs for the organisation's key systems, and evidence that these have been agreed with the business.

# Standard 7: Assertion 3

Mandatory

## Evidence Item 7.3.5

You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary

All emergency contacts are kept securely, in hardcopy and are up-to-date

Draft press materials for data security incidents are ready

Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed

**Your organisation tests its backups regularly to ensure it can restore from a backup.**

Your organisation's backups are kept securely and separate from your network ('offline'), or in a cloud service designed for this purpose.

### Control Objective

The organisation makes backups of all of the data required to effectively recover its key services. These backups are tested on a regular basis (at least annually). The backups referred to in this evidence item are to facilitate full system restores, not ad-hoc file restoration requests.

### Approach

1. Review documentation associated with the organisation's previous restore from backup and determine if the restore was performed in line with its policies and procedures.

### Assessment Documentation

1. Documentation associated with the organisation's previous restore from backup.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 7: Assertion 3

Mandatory

## Evidence Item 7.3.6

You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary

All emergency contacts are kept securely, in hardcopy and are up-to-date

Draft press materials for data security incidents are ready

Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed

Your organisation tests its backups regularly to ensure it can restore from a backup.

**Your organisation's backups are kept securely and separate from your network ('offline'), or in a cloud service designed for this purpose.**

### Control Objective

With at least one separate backup offline at any given time, an incident cannot affect all backups simultaneously and hence reducing the likelihood that an organisation will be unable to effectively recover its key services.

### Approach

1. Determine if multiple backups exists for critical data and if so, determine where these are stored and if any of these are offline e.g. only connecting the backup to live systems when absolutely necessary. Standard good practice for creating resilient data backups is to follow the '3-2-1' rule; at least 3 copies, on 2 devices, and 1 offsite. (Further guidance at https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world )

### Assessment Documentation

1. Backup policy

# Standard 8 - Unsupported Systems

The NHS Big Picture Guidance

No unsupported operating systems, software or internet browsers are used within the IT estate.
**Typical departments responsible for this standard:** IT Security, Data Security and Protection

## Overview of standard

### Assertion 1

All software and hardware has been surveyed to understand if it is supported and up to date.

### Assertion 2

Unsupported software and hardware is categorised and documented, and data security risks are identified and managed.

### Assertion 3

Supported systems are kept up-to-date with the latest security patches.

### Assertion 4

You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.

Back

# Standard 8: Assertion 1

All software and hardware has been surveyed to understand if it is supported and up to date.

## Objective

Having a detailed understanding of an organisation's IT landscape, enables it to have oversight of security vulnerabilities across its technologies, including; infrastructure, operating system, database and application level vulnerabilities. This understanding underpins the organisation's ability to assess and subsequently mitigate its security vulnerabilities.

**Category 2**

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 8: Assertion 1

## Evidence Item 8.1.1

All software and hardware has been surveyed to understand if it is supported and up to date.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Provide evidence of how the organisation tracks and records all software assets and their configuration.

The organisation tracks and records all end user devices and removable media assets.

The organisation ensures that software that is no longer within support or receiving security updates is uninstalled. Where this is impractical, the endpoint should be isolated and have limited connectivity to the network.

### Control Objective

The organisation effectively manages its software assets and their configuration such that vulnerabilities can be identified, managed and remediated - where appropriate and proportionate to risk - in a timely manner.

### Approach

1. Determine if the organisation has a documented process for managing software assets. Review this process and assess if it requires a list of software assets to be managed centrally, with version numbers included. There should also be a mechanism for updating this asset register to reflect changes in the organisation's application landscape.

2. Review the software asset register and determine whether it is in line with the organisation's software asset management process, containing a central list of all software assets with version numbers included.

3. Assess if the organisation receives assurance over the completeness and accuracy of its software asset register. This could include a manual or automated review. Review evidence of a sample of software asset register reviews.

4. Determine if the organisation has a central software deployment mechanism to prevent the installation of unlicensed/unauthorised software. Review evidence associated with this central deployment mechanism.

Continued

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 8: Assertion 1

## Evidence Item 8.1.1

All software and hardware has been surveyed to understand if it is supported and up to date.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Provide evidence of how the organisation tracks and records all software assets and their configuration.

The organisation tracks and records all end user devices and removable media assets.

The organisation ensures that software that is no longer within support or receiving security updates is uninstalled. Where this is impractical, the endpoint should be isolated and have limited connectivity to the network.

### Assessment Documentation

1. Software asset management policy.
2. Software asset register.
3. Evidence associated with a sample of software asset register reviews.
4. Evidence associated with the organisation's central software deployment mechanism.

Previous

# Standard 8: Assertion 1

## Evidence Item 8.1.2

All software and hardware has been surveyed to understand if it is supported and up to date.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Provide evidence of how the organisation tracks and records all software assets and their configuration.

**The organisation tracks and records all end user devices and removable media assets.**

The organisation ensures that software that is no longer within support or receiving security updates is uninstalled. Where this is impractical, the endpoint should be isolated and have limited connectivity to the network.

### Control Objective

The organisation effectively manages its IT assets (including end user devices and removable media). This reduces the risk of IT assets, and the data that resides on them, being lost without Management becoming aware.

### Approach

1. Determine if the organisation has a documented process for managing IT assets. Review this process and assess if it requires a list of IT assets to be managed centrally, with ownership assigned to individuals. There should also be a mechanism for updating this asset register to reflect changes in the organisation's IT environment.

2. Assess if the organisation receives assurance over the completeness and accuracy of its IT asset register. This could include a manual or automated review. Review evidence of a sample of IT asset register reviews.

### Assessment Documentation

1. IT asset management process.

2. Evidence associated with a sample of IT asset register reviews.

# Standard 8: Assertion 1

## Evidence Item 8.1.4

All software and hardware has been surveyed to understand if it is supported and up to date.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Provide evidence of how the organisation tracks and records all software assets and their configuration.

The organisation tracks and records all end user devices and removable media assets.

**The organisation ensures that software that is no longer within support or receiving security updates is uninstalled. Where this is impractical, the endpoint should be isolated and have limited connectivity to the network.**

### Control Objective

The organisation is managing the risk posed by software which is no longer under vendor support or receiving security updates; either by uninstalling the software or restricting its access to the organisation's network.

### Approach

1. Determine whether the organisation's software asset register includes details of whether the software is within vendor support, or if there is another means of tracking software which is close to/beyond end of life (i.e. is no longer within support/receiving security updates).

2. Through discussion with Management, determine what steps are being taken to mitigate the risk associated with software that it is no longer under vendor support, and whether this is documented (e.g. vulnerability management policy). We would expect this to include a mechanism for such instances of software to be reported and either uninstalled, or other mitigating controls implemented (e.g. restricted network access or implementation of a "safe zone" within network).

3. Review the organisation's software asset register and confirm that it includes details regarding support and maintenance arrangements and whether software is close to/beyond end of life. For a sample of these applications, review whether the software in question has been uninstalled or whether other mitigating controls have been implemented.

Continued

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 8: Assertion 1

## Evidence Item 8.1.4

All software and hardware has been surveyed to understand if it is supported and up to date.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Provide evidence of how the organisation tracks and records all software assets and their configuration.

The organisation tracks and records all end user devices and removable media assets.

**The organisation ensures that software that is no longer within support or receiving security updates is uninstalled. Where this is impractical, the endpoint should be isolated and have limited connectivity to the network.**

### Assessment Documentation

1. Software asset register.
2. Vulnerability management policy.
3. Evidence that software that is no longer under vendor support has either been uninstalled, or had other mitigating controls applied.

Previous

# Standard 8: Assertion 2

Unsupported software and hardware is categorised and documented, and data security risks are identified and managed.

## Objective

Software and hardware that are no longer supported by their vendors (e.g. Windows XP, 7) may contain security vulnerabilities that are not going to be updated/patched. Using such technologies poses a significant security risk to an organisation, therefore it is essential that organisations have implemented a process to; identify, assess and mitigate the associated risk. There may be a valid business reason why unsupported software and hardware may be maintained (e.g. a critical business application that is only compatible with Windows Server 2003, Windows Server 2008 R2 ), however, this should be formally risk accepted by an appropriately individual in the organisation.

**Category 2**

# Standard 8: Assertion 2

## Evidence Item 8.2.1

Unsupported software and hardware is categorised and documented, and data security risks are identified and managed.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

List any unsupported software prioritised according to business risk, with remediation plan against each item.

The SIRO confirms that the overall risks of using unsupported systems are being managed and the scale of unsupported software is reported to your board along with the plans to address.

### Control Objective

The organisation effectively manages unsupported software that no longer receives security updates. Unsupported software is known and quantified; recorded centrally and risk assessed, with remediation plans defined.

### Approach

1. Understand if the organisation has a consolidated list of all of its software that is no longer under vendor support. Review this list and confirm that it includes details on the software and whether there are any known security vulnerabilities. It should also include a risk assessment of the software, with remediation plans defined.

### Assessment Documentation

1. List of out of support software.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 8: Assertion 2

## Evidence Item 8.2.2

Unsupported software and hardware is categorised and documented, and data security risks are identified and managed.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

List any unsupported software prioritised according to business risk, with remediation plan against each item.

The SIRO confirms that the overall risks of using unsupported systems are being managed and the scale of unsupported software is reported to your board along with the plans to address.

### Control Objective

Where out of support software cannot be uninstalled, replaced or otherwise remediated for a valid business reason, risk acceptances are approved at a senior level in the organisation.

### Approach

1. Where remediation is not possible for a valid business reason (for example a business critical application will not run on a supported version of Microsoft Server), there is a mechanism for this to be treated (e.g. mitigating controls implemented), or formally risk accepted at a senior level in the organisation.

2. For a sample of 'out of support software applications; review the evidence of the mitigating control (or risk acceptance) and determine whether it was approved at a senior level in the organisation (e.g. SIRO) and has valid business reasons associated with it (see audit guide for sample size guidance). Check for the sampled applications approach is complaint with the plans that go to the board.

### Assessment Documentation

1. Risk acceptances associated with out of support software that cannot be remediated for a valid business reason.

2. Evidence of mitigating controls designed to treat/reduce the risk associated with unsupported systems.

3. Evidence of an unsupported software plan being reported at board level.

Back

# Standard 8: Assertion 3

Supported systems are kept up-to-date with the latest security patches.

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

## Objective

Consistently applying security patches shortly after they are released by the vendor, is an important control in minimising the number of security vulnerabilities in an organisation's IT environment. This helps reduce the 'attack surface' of an organisation.

**Category 2**

# Standard 8: Assertion 3

## Evidence Item 8.3.1

Supported systems are kept up-to-date with the latest security patches.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

**How do your systems receive updates and how often?**

How often, in days, is automatic patching typically being pushed out to remote endpoints?

There is a documented approach to applying security updates (patches) agreed by the SIRO.

Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.

Where a security patch has been classed as critical or high-risk vulnerability has not been applied, explain the technical remediation and risk management that has been undertaken.

8.3 Continued

### Control Objective

The organisation has a patch management procedure that enables security patches to be applied at the operating system, database, application and infrastructure levels.

### Approach

1. Determine if the organisation has a patch management procedure and/or strategy/policy. Review the document and determine if it includes the frequency and scope of its patch management controls.

2. Review the scope of the organisation's patch management controls, and confirm that it includes the operating system, database, application and infrastructure levels. It should also include Microsoft and third party (e.g. Java) patches.

3. Determine if there is regular reporting to Management on patch status, to give them oversight of the effectiveness of the organisation's patch management activities.

4. For a sample of endpoints (including servers), review operating system and application patching schedules to confirm that patches are scheduled to be applied in line with policy. Review installation logs to confirm that historic patches have been applied.

### Assessment Documentation

1. Patch management procedure and/or strategy/policy.

2. Patch management reporting.

3. Sample of operating system and application patching schedules.

4. Sample of change and installation logs to confirm that historic patches have been applied.

# Standard 8: Assertion 3

## Evidence Item 8.3.2

Supported systems are kept up-to-date with the latest security patches.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

How do your systems receive updates and how often?

How often, in days, is automatic patching typically being pushed out to remote endpoints?

There is a documented approach to applying security updates (patches) agreed by the SIRO.

Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.

Where a security patch has been classed as critical or high-risk vulnerability has not been applied, explain the technical remediation and risk management that has been undertaken.

8.3 Continued

### Control Objective

The organisation has the capability to automatically deploy patches to remote endpoints, for example, laptops and mobile devices.

### Approach

1. Review the scope of the organisation's patch management controls, and confirm that it includes automatically pushing patches to remote endpoints.

2. Assess whether the organisation's patch management technology configurations in this area are in line with the patch management procedure and/or strategy/policy, and the organisation's response to this evidence item in the DSP Toolkit.

3. If not tested separately, complete approach step 3 in 8.3.1.

### Assessment Documentation

1. Patch management procedure and/or strategy/policy.

2. Patch management technology configurations.

# Standard 8: Assertion 3

## Evidence Item 8.3.3

Supported systems are kept up-to-date with the latest security patches.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

How do your systems receive updates and how often?

How often, in days, is automatic patching typically being pushed out to remote endpoints?

There is a documented approach to applying security updates (patches) agreed by the SIRO.

Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.

Where a security patch has been classed as critical or high-risk vulnerability has not been applied, explain the technical remediation and risk management that has been undertaken.

8.3 Continued

### Control Objective

Patches for critical or high-risk vulnerabilities are deployed to the live environment no later than 14 days after the day of release.

### Approach

1. Determine whether the organisation has an approach for identifying and deploying critical and/or high-risk security patches outside of the normal patching schedule. For example, Common Vulnerability Scoring System (CVSS) scores of 7 or greater should be considered for patching / remediation as a priority; and should be considered alongside the organisation's risk and threat profile, nature of services, the value of information assets / impact of a breach and good practice in vulnerability remediation - i.e. what is the justification for not remediating vulnerabilities of CVSS 7 or higher?

2. Review this process and confirm that it is designed so that patches for critical and high-risk vulnerabilities are applied within 14 days of release.

3. For a sample of CareCERT alerts, review evidence that the vulnerability has been managed and remediated in a timely manner. Where there was a valid business reason not to remediate the vulnerability, this should be formally documented and risk accepted.

### Assessment Documentation

1. Patch management procedure and/or strategy/policy.

Back

# Standard 8: Assertion 3

## Evidence Item 8.3.4

Supported systems are kept up-to-date with the latest security patches.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

How do your systems receive updates and how often?

How often, in days, is automatic patching typically being pushed out to remote endpoints?

There is a documented approach to applying security updates (patches) agreed by the SIRO.

**Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.**

Where a security patch has been classed as critical or high-risk vulnerability has not been applied, explain the technical remediation and risk management that has been undertaken.

8.3 Continued

### Control Objective

Patches for critical or high-risk vulnerabilities, that have not been applied within 14 days, are reported to the SIRO for either risk acceptance or escalation with a view to remediation.

### Approach

1. Determine whether the organisation reports patch status to Management on a regular basis.

2. Assess whether there is a process by which patches designed to mitigate critical or high-risk vulnerabilities, that have not been patched within 14 days of being released, are escalated to the SIRO for risk acceptance or remediation.

3. Review a sample of risk acceptances and determine for each whether the risk associated with not patching the vulnerability is properly documented, assessed and accepted by the organisation's SIRO. Review the organisation's data security and protection related risk acceptances and determine if the volume of risk acceptances appears to be appropriate.

### Assessment Documentation

1. Example patch status report.

2. Sample of SIRO risk acceptances.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 8: Assertion 3

## Evidence Item 8.3.5

Supported systems are kept up-to-date with the latest security patches.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

How do your systems receive updates and how often?

How often, in days, is automatic patching typically being pushed out to remote endpoints?

There is a documented approach to applying security updates (patches) agreed by the SIRO.

Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.

Where a security patch has been classed as critical or high-risk vulnerability has not been applied, explain the technical remediation and risk management that has been undertaken.

8.3 Continued

### Control Objective

The organisation has a process in place to ensure that where security patches for critical or a high risk vulnerabilities have not been applied within 14 days, technical remediation and risk management is in place.

### Approach

1. Determine how the organisation deals with high risk vulnerabilities where a patch has not been applied.

2. Assess whether there is a process to determine why a patch cannot be applied and how it blends technical remediation and risk mitigation.

3. Review a sample of patches that been determined to be treated by technical remediation and / or risk managed. associated. Determine if the reasons behind the technical remediation and /or risk managed are proportionate. Determine where technical remediations are applied whether this is short terms and a patch will be applied later or more long term.

### Assessment Documentation

1. Example patch status report.

2. Patch process treatment procedure or process

# Standard 8: Assertion 3

## Evidence Item 8.3.6

Supported systems are kept up-to-date with the latest security patches.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation is actively using and managing Advanced Threat Protection (ATP) and regularly reviewing alerts from Microsoft defender for endpoint.

95% of your organisation's server estate and 98% of your desktop estate are on supported versions of operating systems.

Your organisation is registered for and actively using the NCSC early warning service.

8.3 Previous

### Control Objective

The organisation has the technology and processes in place to actively manage ATP. This could be facilitated by the NHS England Endpoint Detection and Response capability, or another solution and/or service designed to mitigate Advanced Persistent Threats (APTs).

### Approach

1. Determine if the organisation has technology and/or processes for managing ATP. Review evidence of the control implementation, for example, reports from the ATP solution if applicable. Review the configuration of a sample of ATP technologies and understand how Indicators of Compromise (IoCs) are defined, and whether the appropriate specialists are engaged / consulted when defining IoCs.

2. If the organisation does not currently have any controls in this area, but has plans to implement some, review the IT security strategy and determine if the implementation of an ATP solution is included.

3. Understand if the organisation has a measure to assess its overall exposure to known threats and vulnerabilities e.g. Exposure score in ATP solution, e.g. aggregate view of CVSS (Common Vulnerability Scoring System) assessments.

### Assessment Documentation

1. Evidence of implementation of ATP solution.

2. IT security strategy for references to ATP solution.

# Standard 8: Assertion 3

## Evidence Item 8.3.7

Supported systems are kept up-to-date with the latest security patches.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation is actively using and managing Advanced Threat Protection (ATP) and regularly reviewing alerts from Microsoft defender for endpoint.

**95% of your organisation's server estate and 98% of your desktop estate are on supported versions of operating systems.**

Your organisation is registered for and actively using the NCSC early warning service.

8.3 Previous

### Control Objective

The organisation's server and desktop estates run supported operating systems.

### Approach

1. Determine how the organisation records its desktop and server assets.
2. From the Microsoft Defender for Endpoint (MDE) / Advanced Threat Protection (ATP) dashboard / equivalent review the percentage of servers and desktops on supported versions of operating systems.
3. Review and analyse reporting from the organisation's asset register and recent discovery audits to determine whether the supported system rate matches the response provided by the organisation, and whether this is greater than 95% for servers and 98% for desktops. This should include a walk through and analysis of how the result was calculated with a relevant individual from the Data Security and Protection team, consider whether this includes all applicable assets and not just a subset.

### Assessment Documentation

1.Hardware asset registers

2.Recent discovery audit

Back

# Standard 8: Assertion 3

## Evidence Item 8.3.8

Supported systems are kept up-to-date with the latest security patches.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation is actively using and managing Advanced Threat Protection (ATP) and regularly reviewing alerts from Microsoft defender for endpoint.

95% of your organisation's server estate and 98% of your desktop estate are on supported versions of operating systems.

Your organisation is registered for and actively using the NCSC early warning service.

8.3 Previous

### Control Objective

The organisation has controls in place to identify and manage potential compromise in a timely fashion. The National Centre for Cyber Security (NCSC) provides a free service. This is based on intelligence feeds and specific vulnerability alerts.

### Approach

1. Through discussion with Management, understand if the organisation has signed up to the service.
2. Review evidence of the control implementation. the NCSC early alert service, review the dashboard that outlines the systems being monitored along with any vulnerabilities that have been identified. Review the early warning report for the organisation's external systems to see if intelligence, events or alerts are being actioned (this should in conjunction with other services such as NCSC Web check and the NHS Cyber Alerts.

### Assessment Documentation

1. Evidence associated with the early warning systems and outputs.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 8: Assertion 4

You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.

## Objective

By having a centralised vulnerability management process, an organisation has oversight of its critical/high risk security vulnerabilities and is able to patch the vulnerability (if one is available), or implement mitigating controls such as network segmentation to reduce the risk posed by the vulnerability.

**Category 2**

# Standard 8: Assertion 4

## Evidence Item 8.4.1

You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation's infrastructure is protected from common cyber-attacks through secure configuration and patching?

All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.

You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.

### Control Objective

The organisation has the processes and technology to patch its IT infrastructure on a continuous basis. This reduces the risk of a security vulnerability being exploited by a potential threat actor, resulting in a data security or data protection incident. In addition, the organisation has an understanding of its key cyber security threats based on both its industry, and the nature of the services it provides and an understanding of how those threats might manifest in an attack and which controls they have in place to address the threats and 'common cyber-attacks.'

### Approach

1. While considering the other in-scope evidence items in Standard 8, determine whether the organisation has the appropriate processes and technologies to secure its infrastructure through secure configuration and patching.

2. Review the organisation's approach towards identifying its key cyber security threats, including whether it leveraged industry good practice (such as guidance from the National Cyber Security Centre, NCSC).

### Assessment Documentation

1. Documentation associated with the organisation's secure configuration and patching controls.

2. Threat intelligence sources the organisation has used to identify its key cyber security threats.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 8: Assertion 4

## Evidence Item 8.4.2

You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation's infrastructure is protected from common cyber-attacks through secure configuration and patching?

All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.

You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.

### Control Objective

The organisation has the processes and technology to patch its IT infrastructure on a continuous basis. This reduces the risk of a security vulnerability being exploited by a potential threat actor, resulting in a data security and protection incident.

### Approach

1. In order to test this evidence item, the testing approach for the following evidence items should be followed:
8.1.1, 8.1.4, 8.2, 8.3.1-8.3.4

### Assessment Documentation

1. In order to test this evidence item, see the assessment documentation for the following evidence items:
8.1.1, 8.1.4, 8.2, 8.3.1-8.3.4

# Standard 8: Assertion 4

## Evidence Item 8.4.3

You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation's infrastructure is protected from common cyber-attacks through secure configuration and patching?

All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.

You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.

### Control Objective

The organisation has a vulnerability management process that outlines how the organisation identifies and effectively manages vulnerabilities through to remediation.

### Approach

1. Determine and review, if applicable, the organisation's vulnerability management process. Assess if this includes details on how vulnerabilities are identified; assessed; and managed through to remediation and/or risk acceptance. Review whether there is a requirement to perform regular internal and external network vulnerability scans for all publicly facing infrastructure. Request and review a sample of these vulnerability scan reports.

2. Determine if the organisation maintains a central record of its hardware and software security vulnerabilities. Request and review this record. For a sample of CareCERT alerts, review evidence that the vulnerability has been managed and remediated in a timely manner. Where there was a valid business reason not to remediate the vulnerability, this should be formally documented and risk accepted.

### Assessment Documentation

1. Vulnerability management process.

2. Sample of vulnerability scanning reports.

3. List of the organisation's security vulnerabilities.

# Standard 9 - IT Protection

The NHS Big Picture Guidance

A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

**Typical departments responsible for this standard:** IT, IT Security, Data Security and Protection, Legal

## Overview of standard

### Assertion 1

All networking components have had their default passwords changed.

### Assertion 2

A penetration test has been scoped and undertaken.

### Assertion 3

Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.

### Assertion 4

You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services.

### Assertion 5

You securely configure the network and information systems that support the delivery of essential services.

### Assertion 6

The organisation is protected by a well managed firewall

Back

# Standard 9: Assertion 1

All networking components have had their default passwords changed.

## Objective

If an organisation does not change the passwords of its network components from their default values, there is a risk that this could be exploited by a threat actor, potentially resulting in the compromise of critical infrastructure.

**Category 2**

# Standard 9: Assertion 1

## Evidence Item 9.1.1

All networking components have had their default passwords changed.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

The Head of IT, or equivalent role, confirms all networking components have had their default passwords changed to a high strength password.

The Head of IT, or equivalent role confirms all the devices have had their default passwords changed.

### Control Objective

Network components have their administrative passwords changed from the vendor-supplied default passwords to help prevent a threat actor from being able to gain administrative access to the devices.

### Approach

1. Determine if the organisation has a documented process for deploying network components. Review this process and determine if there is a requirement/step to change the administrative passwords from their default values.

2. Understand if the organisation has implemented a privileged access management solution, which could be used to manage network infrastructure administrative passwords. Review the configuration of this solution (if applicable), and determine if it is used for managing the administrative passwords on these devices.

### Assessment Documentation

1. Network component deployment process.

2. Privileged access management solution configurations.

3. Pen Test and Network monitoring software

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 9: Assertion 1

## Evidence Item 9.1.2

All networking components have had their default passwords changed.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

The Head of IT, or equivalent role, confirms all networking components have had their default passwords changed to a high strength password.

The Head of IT, or equivalent role confirms all the devices have had their default passwords changed.

### Control Objective

There is a requirement for the organisation's end user device passwords to be changed from their default values.

### Approach

1. Request and review the organisation's password policy. Determine if there is a requirement for the organisation to change its end user device passwords on a regular basis.

2. Review the organisation's password configuration settings and determine whether there is a requirement for passwords to be reviewed on a regular basis.

3. Request and review a sample of recent penetration test reports and determine whether any exceptions were noted relating to default passwords or old passwords outside policy parameters are being used across the organisation.

### Assessment Documentation

1. Password policy.

2. End user device password configurations.

3. Sample of penetration test reports.

Back

# Standard 9: Assertion 2

A penetration test has been scoped and undertaken.

## Objective

Organisations should have a number of mechanisms to receive assurance over its technical controls to protect against and detect cyber security attacks. One of these should be both internal and external penetration testing/ethical hacking, and vulnerability scans. Penetration tests should be repeated on at least an annual basis, and vulnerabilities identified should be managed and remediated in a timely manner.

**Category 2**

# Standard 9: Assertion 2

## Evidence Item 9.2.1

A penetration test has been scoped and undertaken.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

The annual IT penetration testing is scoped in negotiation between the SIRO, business and testing team including a vulnerability scan and checking that all networking components have had their default passwords changed to a high strength password.

The SIRO or equivalent senior role has reviewed the results of latest penetration testing, with an action plan for its findings.

### Control Objective

The scope of the organisation's annual penetration test is defined and approved by relevant accountable and responsible individuals from across the organisation. The test includes a network vulnerability scan and a review of network appliance passwords.

### Approach

1. Through discussion with Management, understand how the scope of the annual penetration test is agreed. Review evidence associated with the scope being agreed, and determine whether it includes the SIRO and representatives from the business, as well as the penetration testing team.

2. Review the scope of the organisation's previous penetration test and determine whether it includes a network vulnerability scans, as well as a review of network appliance passwords.

### Assessment Documentation

1. Penetration testing scope from previous penetration test report.

2. Evidence that the scope was agreed by the SIRO and representatives from the business, as well as the penetration testing team.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 9: Assertion 2

## Evidence Item 9.2.3

A penetration test has been scoped and undertaken.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

The annual IT penetration testing is scoped in negotiation between the SIRO, business and testing team including a vulnerability scan and checking that all networking components have had their default passwords changed to a high strength password.

The SIRO or equivalent senior role has reviewed the results of latest penetration testing, with an action plan for its findings.

### Control Objective

The SIRO reviews / receives / is suitably briefed on the organisation's penetration test reports. Action plans are defined for any security vulnerabilities identified.

### Approach

1. Determine whether the SIRO has reviewed the organisation's previous penetration test report.

2. Confirm that action plans have been defined, and approved by an appropriate individual in the organisation, for application security vulnerabilities identified.

### Assessment Documentation

1. Evidence that the SIRO has reviewed the organisation's previous penetration test report.

2. Evidence that this individual has also approved the action plans associated with mitigating application security vulnerabilities identified.

Back

# Standard 9: Assertion 3

Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.

## Objective

Organisations should ensure that applications processing sensitive data, or supporting key operational services, do not contain security vulnerabilities - including at the code level. There are a number of technical controls that organisations can deploy to enable this, including; application security testing against the Open Web Application Security Project (OWASP) 'top 10' security vulnerabilities, and use of NCSC's web checking service for publicly facing applications. Other technical security controls included in this assertion includes; the management of perimeter firewalls and email encryption.

**Category 2**

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 9: Assertion 3

## Evidence Item 9.3.1

Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.

The organisation has a technology solution or service that prevents users from accessing potentially malicious websites, reducing the risk of the organisation's infrastructure being infected with malware.

The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators.

The organisation understands and records all IP ranges in use across the organisation.

The organisation protects its data in transit (including email) using appropriate technical controls, such as encryption.

9.3 Continued

### Control Objective

The organisation has a secure software development lifecycle (SSDLC) or equivalent software and code security approach in place, aligned to industry good practice such as OWASP, to reduce the risk of code vulnerabilities or web application vulnerabilities being exploited.

### Approach

1. Determine if the organisation has a software development methodology in place. If so, review this methodology and determine whether it contains security requirements in line with industry good practice such as OWASP. The organisation should define security requirements prior to build, and test the application against those requirements prior to go-live.

2. Determine if the individuals in the organisation responsible for software development receive training on secure design principles. Pick a sample of developers and review evidence that they have completed this training.

3. Assess if the organisation has the capability (technology and processes) to perform security testing on web applications prior to go-live. This could include automated code reviews against the OWASP top 10, or web application penetration tests.

Continued

# Standard 9: Assertion 3

## Evidence Item 9.3.1

Mandatory

Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.

The organisation has a technology solution or service that prevents users from accessing potentially malicious websites, reducing the risk of the organisation's infrastructure being infected with malware.

The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators.

The organisation understands and records all IP ranges in use across the organisation.

The organisation protects its data in transit (including email) using appropriate technical controls, such as encryption.

9.3 Continued

### Assessment Documentation

1. Software development methodology that includes security requirements in line with industry good practice such as OWASP.

2. Evidence associated with developers in the organisation completing secure design principles training.

3. Evidence associated with the organisation's capability to perform testing on web application code prior to go-live.

Previous

# Standard 9: Assertion 3

## Evidence Item 9.3.3

Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.

**The organisation has a technology solution or service that prevents users from accessing potentially malicious websites, reducing the risk of the organisation's infrastructure being infected with malware.**

The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators.

The organisation understands and records all IP ranges in use across the organisation.

The organisation protects its data in transit (including email) using appropriate technical controls, such as encryption.

9.3 Continued

### Control Objective

The organisation has a technology solution or service that prevents users from accessing potentially malicious websites, reducing the risk of the organisation's infrastructure being infected with malware. This could include the National Centre for Cyber Security's free DNS service.

### Approach

1. Confirm whether the organisation has implemented a website blocklisting solution to prevent users accessing potentially malicious websites. This could include the NCSC's free DNS service.

2. Review evidence associated with the control implementation. For example, reporting from the solution outlining the number of attempted connections blocked.

### Assessment Documentation

1. Evidence associated with the implementation of the technology solution. This could include reporting from the technology solution outlining the number of attempted connections blocked.

# Standard 9: Assertion 3

## Evidence Item 9.3.4

Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.

The organisation has a technology solution or service that prevents users from accessing potentially malicious websites, reducing the risk of the organisation's infrastructure being infected with malware.

**The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators.**

The organisation understands and records all IP ranges in use across the organisation.

The organisation protects its data in transit (including email) using appropriate technical controls, such as encryption.

9.3 Continued

### Control Objective

Only authorised individuals are able to make changes to the organisation's authoritative DNS entries to prevent domain addresses being pointed toward potentially malicious IP addresses.

### Approach

1. Confirm with Management that access to the organisation's authoritative DNS server is restricted, and that access requests to this server are reviewed by an appropriate individual.

2. Determine how administrators access the organisation's authoritative DNS server, and whether multi-factor authentication / strong authentication is used.

3. Request the list of individuals that have access to the organisation's authoritative DNS server. Pick a sample of these and review evidence that their access was approved by an appropriate individual.

4. Confirm whether access to this server is reviewed on a regular basis. Where a regular review is conducted, request evidence of the previous three reviews.

### Assessment Documentation

1. Access management process

2. List of users with access to the organisation's authoritative DNS server.

3. Evidence that a sample of individuals had access to the server approved.

4. Evidence of regular access reviews on the authoritative DNS server.

# Standard 9: Assertion 3

## Evidence Item 9.3.5

Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.

The organisation has a technology solution or service that prevents users from accessing potentially malicious websites, reducing the risk of the organisation's infrastructure being infected with malware.

The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators.

**The organisation understands and records all IP ranges in use across the organisation.**

The organisation protects its data in transit (including email) using appropriate technical controls, such as encryption.

9.3 Continued

### Control Objective

The organisation has visibility of its entire IT infrastructure and effectively manages its IP address ranges.

### Approach

1. Determine if the organisation has a consolidated record of all the IP ranges in use across its network. Request and review this record.

2. Assess whether the organisation has a mechanism for regularly reviewing this record, updating it when new IP ranges are brought in to its infrastructure, or legacy ranges removed. Review evidence of the previous three reviews (automated or manual).

### Assessment Documentation

1. Consolidated record of IP ranges across the organisation's network.

2. Evidence of IP range reviews (automated or manual).

# Standard 9: Assertion 3

## Evidence Item 9.3.6

Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.

The organisation has a technology solution or service that prevents users from accessing potentially malicious websites, reducing the risk of the organisation's infrastructure being infected with malware.

The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators.

The organisation understands and records all IP ranges in use across the organisation.

**The organisation protects its data in transit (including email) using appropriate technical controls, such as encryption.**

9.3 Continued

### Control Objective

All data in transit across the organisation is encrypted using the TLS 1.2 protocol or later to protect the confidentiality of its key data.

### Approach

1. Request and review the organisation's encryption strategy to determine if there is a requirement for data in transit to be encrypted using the TLS 1.2 protocol or later.

2. Review the organisation's browser and email configurations to confirm that TLS 1.2 is enabled in line with its encryption policy (if applicable). Email configurations should not be tested if the organisation uses NHSmail.

### Assessment Documentation

1. Encryption policy.

2. Browser and email configurations.

# Standard 9: Assertion 3

## Evidence Item 9.3.7

Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

The organisation has registered and uses the National Cyber Security Centre (NCSC) Web Check service, or equivalent web check service, for its publicly-visible applications.

The organisation maintains a register of medical devices connected to its network.

What is the organisation's data security assurance process for medical devices connected to the network.

9.3 Previous

### Control Objective

The organisation has controls in place to identify and manage vulnerabilities in its publicly facing websites. The National Centre for Cyber Security (NCSC) provides a free web check service that can be used by public sector bodies for this purpose. Other options include using an External Managed Service or Integrated Service Function.

### Approach

1. Through discussion with Management, understand if the organisation has any technical controls in place to identify and manage vulnerabilities on its publicly facing websites.

2. Review evidence of the control implementation. For example, for the NCSC web check service, review the dashboard that outlines the websites being monitored along with any vulnerabilities that have been identified. Review the web check service report for the organisation's external website and determine if it identifies any vulnerabilities that are not currently being managed.

### Assessment Documentation

1. Evidence associated with website monitoring solution, vulnerability reporting for example.

# Standard 9: Assertion 3

## Evidence Item 9.3.8

Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

The organisation has registered and uses the National Cyber Security Centre (NCSC) Web Check service, or equivalent web check service, for its publicly-visible applications.

**The organisation maintains a register of medical devices connected to its network.**

What is the organisation's data security assurance process for medical devices connected to the network.

9.3 Previous

### Control Objective

The organisation understands which medical devices are connected to its network

### Approach

1. Request and review the organisation's connected medical device register*
2. Through discussion discovery how the organisation approaches supplier maintenance, network segmentation and whether 3rd party access is allowed / managed.
3. Sample a number of devices from the asset register to see if the record reflects current status.

### Assessment Documentation

1. Connected medical devices register
2. Network diagrams
3. Maintenance agreements / statements

* This may be separate register or form part of a larger asset register

# Standard 9: Assertion 3

## Evidence Item 9.3.9

Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

The organisation has registered and uses the National Cyber Security Centre (NCSC) Web Check service, or equivalent web check service, for its publicly-visible applications.

The organisation maintains a register of medical devices connected to its network.

What is the organisation's data security assurance process for medical devices connected to the network.

9.3 Previous

### Control Objective

The organisation manages the data security lifecycle of a medical device

### Approach

1. Review the organisations medical devices data security policy / procedure to ensure it cover the entire lifecycle of the device (from commissioning to retirement). How medical device data security is measured and protected.

2. Confirm that the policy / procedure takes into account emerging medical device technology and is in line with current guidance,

### Assessment Documentation

1. Medical devices data security policy / procedure

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 9: Assertion 4

You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services.

## Objective

The objective of this assertion is to assess whether the organisation receives an appropriate level of assurance over the design and operating effectiveness of its data security and protection control environment. This is essential in enabling the continuous improvement in the maturity of the organisation's security controls.

**Category 2**

# Standard 9: Assertion 4

## Evidence Item 9.4.1

You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

You validate that the security measures in place to protect the networks and information systems are effective, and remain effective for the lifetime over which they are needed.

Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.

Your organisation has completed an independent audit of your Data Security and Protection Toolkit and has reported the results to the Board.

### Control Objective

As part of security technology implementation projects, the organisation considers the assurance requirements of the relevant solutions/infrastructure, and deploys security measures to protect the networks and information systems, regularly reviewing fitness for purpose and effectiveness, over the lifetime of the technology / contract.

### Approach

1. Understand if the organisation has undertaken a process to map the assurance requirements of its security technologies, and implemented these over the lifetime of the technology.

2. Review evidence of a sample of these assurance activities operating. For example, evidence of firewall ruleset reviews.

### Assessment Documentation

1. Security assurance strategy/plan.

2. Outputs of security assurance activities (e.g. Internal Audit reports).

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 9: Assertion 4

## Evidence Item 9.4.4

You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

You validate that the security measures in place to protect the networks and information systems are effective, and remain effective for the lifetime over which they are needed.

**Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.**

Your organisation has completed an independent audit of your Data Security and Protection Toolkit and has reported the results to the Board.

### Control Objective

The organisation effectively uses the outputs of independent assurance reports to remediate issues and continually improve its data security and data protection control environment.

### Approach

1. Request and review the organisation's security assurance policy/procedure (or equivalent) and confirm that it includes a requirement for all actions identified during independent assessments to be recorded centrally, undergo a risk assessment, and managed through to remediation in a timescale defined by its criticality.

2. Request the record of the organisation's actions resulting from security tests. Pick a sample of these and confirm that they were managed through to remediation in line with the policy. Where there is a valid business reason that the action could not be implemented, this should be risk accepted by an appropriate individual in the organisation.

### Assessment Documentation

1. Security assurance policy/procedure (or equivalent).

2. Record of actions resulting from independent assessments.

3. Evidence associated with these actions being managed through to remediation in line with policy.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 9: Assertion 4

Mandatory

## Evidence Item 9.4.5

You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

You validate that the security measures in place to protect the networks and information systems are effective, and remain effective for the lifetime over which they are needed.

Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.

**Your organisation has completed an independent audit of your Data Security and Protection Toolkit and has reported the results to the Board.**

### Control Objective

The organisation's DSP Toolkit response is reviewed by an independent body to determine whether the response accurately reflects the organisation's data security and protection control environment, and identify any residual risks.

### Approach

1. Review the organisation's previous DSP Toolkit assessment report and confirm that its scope included both; the accuracy of the DSP Toolkit response, and the overall effectiveness of the organisation's DSP Toolkit control environment.

### Assessment Documentation

1. DSP Toolkit Assessment report.

Back

# Standard 9: Assertion 5

You securely configure the network and information systems that support the delivery of essential services.

## Objective

One of the key 'battlegrounds' for cyber security is at the endpoint, with the way in which users interact with the internet frequently being exploited by threat actors. This assertion includes a number of controls designed to mitigate this threat, including; controls to prevent users downloading and installing potentially malicious software on their devices, endpoint hardening, encryption of data at rest and data in transit, and controls to prevent software automatically executing on end user devices.

**Category 2**

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

Back

# Standard 9: Assertion 5

## Evidence Item 9.5.1

You securely configure the network and information systems that support the delivery of essential services.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All devices in your organisation have technical controls that manage the installation of software on the device.

Confirm all data are encrypted at rest on all mobile devices and removable media and you have the ability to remotely wipe and/or revoke access from an end user device.

You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.

End-user devices are built from a consistent and approved base image.

End-user device security settings are managed and deployed centrally.

Auto-run is disabled.

All remote access is authenticated.

9.5 Continued

### Control Objective

Technical controls are implemented that govern what software can be used to help prevent insecure or malicious software being installed on business devices or deployed in the network or IT systems. This could be done by deploying application allow listing technology and/or restricting local administrative access rights.

### Approach

1. Determine if technical controls have been implemented to prevent unauthorised allow listed initially malicious) software from being downloaded and installed without Management oversight.

2. If local administrative rights are blocked, understand how this is enforced and exceptions approved. Review three exceptions and assess whether the reasons provided are appropriate.

3. If application allow listing is in place, review the process by which applications are requested by end users and assessed/approved by the IT team. This process should consider the potential security implications.

### Assessment Documentation

1. Local administrative rights configuration.

2. List of allow listed applications.

3. Local administrative access rights exceptions.

# Standard 9: Assertion 5

## Evidence Item 9.5.2

You securely configure the network and information systems that support the delivery of essential services.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All devices in your organisation have technical controls that manage the installation of software on the device.

**Confirm all data are encrypted at rest on all mobile devices and removable media and you have the ability to remotely wipe and/or revoke access from an end user device.**

You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.

End-user devices are built from a consistent and approved base image.

End-user device security settings are managed and deployed centrally.

Auto-run is disabled.

All remote access is authenticated.

9.5 Continued

### Control Objective

Data on mobile devices (including laptops, smart phones and removable media) is encrypted at rest to prevent the data being read if the device is lost or stolen. In addition, the organisation has the technical capability to remotely delete data from mobile devices and revoke access.

### Approach

1. Determine if the organisation has an encryption policy that outlines its approach to encryption across the organisation.

2. Review the encryption policy and assess if there are controls to encrypt data at rest on mobile devices (including workstations and removable media). *For category 3 and 4 organisations, only health and care data is in scope of this requirement.*

3. Assess if the controls implemented to encrypt the data at rest are in line with good practice, for example, the encryption standards used are appropriate.

4. Review evidence associated with the control implementation, for example, encryption settings/configurations and the decryption screen during laptop boot.

5. Determine if the organisation has implemented a Mobile Device Management (MDM) solution, or other technology, that enables mobile devices to be remotely wiped if they are lost or stolen.

6. Review evidence of MDM implementation.

Continued

# Standard 9: Assertion 5

## Evidence Item 9.5.2

You securely configure the network and information systems that support the delivery of essential services.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All devices in your organisation have technical controls that manage the installation of software on the device.

**Confirm all data are encrypted at rest on all mobile devices and removable media and you have the ability to remotely wipe and/or revoke access from an end user device.**

You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.

End-user devices are built from a consistent and approved base image.

End-user device security settings are managed and deployed centrally.

Auto-run is disabled.

All remote access is authenticated.

9.5 Continued

### Assessment Documentation

1. Encryption policy.
2. Evidence associated with control implementation, for example, encryption settings/configurations and the decryption screen during laptop boot.
3. Evidence associated with MDM implementation.

Previous

# Standard 9: Assertion 5

## Evidence Item 9.5.3

You securely configure the network and information systems that support the delivery of essential services.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All devices in your organisation have technical controls that manage the installation of software on the device.

Confirm all data are encrypted at rest on all mobile devices and removable media and you have the ability to remotely wipe and/or revoke access from an end user device.

**You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.**

End-user devices are built from a consistent and approved base image.

End-user device security settings are managed and deployed centrally.

Auto-run is disabled.

All remote access is authenticated.

9.5 Continued ›

### Control Objective

The organisation has a change management process that prevents changes to its IT environment from being implemented without being approved by the appropriate individuals and security implications being considered.

### Approach

1. Determine if the organisation has a change management procedure and review it to determine if security is considered as part of the approval process.

2. Understand if there are individuals in the information/IT security team that are involved in the organisation's change management processes.

3. Pick a sample of changes and review the associated change documentation to confirm that security has been considered as part of the approval process (see audit guide for sample size).

4. Understand if the organisation has documented network and system configurations, and if there are regular reviews/audits of the actual builds against these standards.

5. Review evidence associated with these reviews/audits.

### Assessment Documentation

1. Change management procedure.

2. Change tickets/approval documentation for a sample of five changes.

3. Documented network and system configurations.

4. Evidence associated with review of network and system configurations against defined standards.

# Standard 9: Assertion 5

## Evidence Item 9.5.5

You securely configure the network and information systems that support the delivery of essential services.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All devices in your organisation have technical controls that manage the installation of software on the device.

Confirm all data are encrypted at rest on all mobile devices and removable media and you have the ability to remotely wipe and/or revoke access from an end user device.

You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.

**End-user devices are built from a consistent and approved base image.**

End-user device security settings are managed and deployed centrally.

Auto-run is disabled.

All remote access is authenticated.

9.5 Continued

### Control Objective

The organisation's end user devices are deployed from a standard build to ensure that security controls are applied consistently across the organisation. The standard builds are documented and reviewed on a regular basis.

### Approach

1. Determine if the organisation has documented standards for end user devices that are applied as part of the device provisioning process.

2. Request and review the documented standards for end user devices.

3. Review if the organisation regularly reviews actual device configurations against the documented standards. If these reviews take place, obtain evidence associated with the previous 3 reviews.

4. Select a random end user device and confirm that it is configured in line with the standard build.

### Assessment Documentation

1. Standards for end user devices.

2. Evidence associated with reviews of actual device configurations against the documented standards.

# Standard 9: Assertion 5

## Evidence Item 9.5.6

You securely configure the network and information systems that support the delivery of essential services.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All devices in your organisation have technical controls that manage the installation of software on the device.

Confirm all data are encrypted at rest on all mobile devices and removable media and you have the ability to remotely wipe and/or revoke access from an end user device.

You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.

End-user devices are built from a consistent and approved base image.

**End-user device security settings are managed and deployed centrally.**

Auto-run is disabled.

All remote access is authenticated.

9.5 Continued

### Control Objective

The organisation's end user devices are deployed from a standard build to ensure that security controls are applied consistently across the organisation. The standard builds are documented and reviewed on a regular basis.

### Approach

1. Determine if the organisation has documented standards for end user devices that are applied as part of the device provisioning process.

2. Request and review the documented standards for end user devices.

3. Review if the organisation regularly reviews actual device configurations against the documented standards. If these reviews take place, obtain evidence associated with the previous 3 reviews.

4. Select a random end user device and confirm that it is configured in line with the standard build.

### Assessment Documentation

1. Standards for end user devices.

2. Evidence associated with reviews of actual device configurations against the documented standards.

Back

# Standard 9: Assertion 5

## Evidence Item 9.5.7

You securely configure the network and information systems that support the delivery of essential services.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All devices in your organisation have technical controls that manage the installation of software on the device.

Confirm all data are encrypted at rest on all mobile devices and removable media and you have the ability to remotely wipe and/or revoke access from an end user device.

You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.

End-user devices are built from a consistent and approved base image.

End-user device security settings are managed and deployed centrally.

**Auto-run is disabled.**

All remote access is authenticated.

9.5 Continued

### Control Objective

Auto-run is disabled across the organisation's IT estate to prevent potentially malicious files from executing without input from the user.

### Approach

1. Through discussion with Management, determine if the organisation has a documented policy or procedure that mandates the disabling of auto-run where possible.

2. Review Operating System (OS) configurations and confirm that auto-run has been disabled in line with policy (if relevant).

### Assessment Documentation

1. Policy/procedure stating that auto-run should be disabled.

2. Auto-run configurations.

Back

# Standard 9: Assertion 5

## Evidence Item 9.5.8

You securely configure the network and information systems that support the delivery of essential services.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

All devices in your organisation have technical controls that manage the installation of software on the device.

Confirm all data are encrypted at rest on all mobile devices and removable media and you have the ability to remotely wipe and/or revoke access from an end user device.

You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.

End-user devices are built from a consistent and approved base image.

End-user device security settings are managed and deployed centrally.

Auto-run is disabled.

All remote access is authenticated.

9.5 Continued

### Control Objective

Remote access to the organisation's corporate network is secured via multi-factor authentication (MFA). This includes web applications, remote access to corporate networks and supplier access, as well as supplier-hosted and ‘software-as-a-service’ applications.

### Approach

1. Determine if the organisation has a technology to support the secure authentication of remote users to its corporate network.

2. Review the technology configuration and determine whether it is configured to enforce secure authentication e.g. MFA.

### Assessment Documentation

1. Remote access technology configurations.

Back

# Standard 9: Assertion 5

## Evidence Item 9.5.9

You securely configure the network and information systems that support the delivery of essential services.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

You have a plan for protecting devices that are natively unable to connect to the Internet, and the risk has been assessed, documented, accepted, reviewed regularly and signed off by the SIRO.

Your organisation meets the secure email standard.

9.5 Previous

### Control Objective

With the proliferation of connected devices in the medical industry, the organisation has a documented approach for how it secures these devices including logical separation.

### Approach

1. Through discussion with Management, determine if the organisation has documented an approach for managing the security risks associated with connected devices and has visibility of the device types along with images/builds/versions/operating systems in use.

2. Review this document (if applicable) and confirm if it considers the appropriate mitigating controls, including logical separation from the corporate network.

### Assessment Documentation

1. Documented approach for managing the security risks associated with connected devices.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 9: Assertion 5

## Evidence Item 9.5.10

You securely configure the network and information systems that support the delivery of essential services.

**Category**

2

You have a plan for protecting devices that are natively unable to connect to the Internet, and the risk has been assessed, documented, accepted, reviewed regularly and signed off by the SIRO.

Your organisation meets the secure email standard.

9.5 Previous

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

### Control Objective

Emails sent to and from health and social care organisations must meet the secure email standard (DCB1596) so that everyone can be sure that sensitive and confidential information is kept secure.

### Approach

1. Determine if the organisation is already operating a compliant service such as NHSmail or Microsoft Office 365 for all staff within their organisation.

2. If the organisation is using NHSmail or Microsoft Office 365 for all staff within their organisation, determine if the organisation has completed all necessary configuration requirements outlined in NHS England Secure Email Standard.

3. If the organisation is not using NHSmail or Office 365, then the organisation must be able to demonstrate their own service is compliant with NHS England Secure Email Standard and has followed NHS England's Secure Email Accreditation Process.

Continued

# Standard 9: Assertion 5

## Evidence Item 9.5.10

You securely configure the network and information systems that support the delivery of essential services.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

You have a plan for protecting devices that are natively unable to connect to the Internet, and the risk has been assessed, documented, accepted, reviewed regularly and signed off by the SIRO.

Your organisation meets the secure email standard.

9.5 Previous

### Assessment Documentation

For organisations using NHSmail or Microsoft Office 365:

1. Process in place to notify the NHSmail team upon becoming aware of any breach of security, including an actual, potential or attempted breach of, or threat to, the security policy and / or the security of the services or the systems used to provide the services.
2. Policies and procedures for the use of secure email using mobile devices and ensure the email service enforces them.
3. Any evidence to demonstrate compliance with the provisions of DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems.
4. Policies and procedures for staff who use the secure email service.
5. Where necessary, evidence to show organisation has followed migration guidance on the NHSmail support site.
6. For organisations using Microsoft Office 365, accreditations must include confirmation that the email service has been configured to securely communicate with NHSmail.

For organisation's not using NHSmail or Microsoft Office365, please also request:

7. Submission of a signed self-accreditation statement, with evidence
8. Evidence checked by the NHS England Data Security Centre and NHSmail team
9. Rectification of findings and re-submission to the NHSmail team

DCB1596 met.

Previous

Back

# Standard 9: Assertion 6

The organisation is protected by a well managed firewall.

## Objective

The purpose of this assertion is to assess whether an organisation has implemented, and effectively manages, firewalls at its network perimeter. This should include all network ingress/egress points. An effectively configured and managed firewall blocks unauthenticated inbound connections by default to prevent unauthorised, and potentially malicious, network connections from being made.

**Category 2**

# Standard 9: Assertion 6

## Evidence Item 9.6.1

The organisation is protected by a well managed firewall.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

One or more firewalls (or similar network device) have been installed on all the boundaries of the organisation's internal network(s).

The administrative interface used to manage the boundary firewall has been configured such that; it is not accessible from the Internet, it requires second factor authentication or is access limited to a specific address.

The organisation has checked and verified that firewall rules ensure that all unauthenticated inbound connections are blocked by default.

All inbound firewall rules (other than default deny) are documented with business justification and approval by the change management process.

Firewall rulesets are reviewed on a regular basis. Rulesets are removed/disabled when they are no longer required.

All of your organisation’s desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by default.

### Control Objective

The organisation has deployed firewalls (or similar network device) at each of its network ingress/egress points to control the network connections into and out of the organisation's corporate network.

### Approach

1. Through discussion with Management and review of a high-level network diagram, confirm that firewalls have been deployed at each of the organisation's network ingress/egress points.

### Assessment Documentation

1. Network diagram.
2. Evidence of firewall implementation, firewall alerts for example.
3. Discovery software results

Back

# Standard 9: Assertion 6

## Evidence Item 9.6.2

The organisation is protected by a well managed firewall.

**Mandatory**

| Category |
| --- |
| 2 |

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

One or more firewalls (or similar network device) have been installed on all the boundaries of the organisation's internal network(s).

**The administrative interface used to manage the boundary firewall has been configured such that; it is not accessible from the Internet, it requires second factor authentication or is access limited to a specific address.**

The organisation has checked and verified that firewall rules ensure that all unauthenticated inbound connections are blocked by default.

All inbound firewall rules (other than default deny) are documented with business justification and approval by the change management process.

Firewall rulesets are reviewed on a regular basis. Rulesets are removed/disabled when they are no longer required.

All of your organisation’s desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by default.

### Control Objective

The organisation's perimeter firewall management console / administrative functionality is not accessible via the internet, preventing threat actors from manipulating the organisation's firewall rulesets or configuration for malicious purposes. If there is a business reason for this administrative console to be connected to the internet, the connection should be secured with multi-factor authentication (MFA) with logging/monitoring and roll-back capability.

### Approach

1. By observing a firewall administrator accessing the administrative console, determine whether this occurs via the internet.

2. Where the console is accessible over the internet, review if MFA is required to access it.

### Assessment Documentation

1. Screenshots outlining the firewall administrator logon procedure.

Back

# Standard 9: Assertion 6

## Evidence Item 9.6.3

The organisation is protected by a well managed firewall.

**Mandatory**

| Category |
| --- |
| 2 |

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

One or more firewalls (or similar network device) have been installed on all the boundaries of the organisation's internal network(s).

The administrative interface used to manage the boundary firewall has been configured such that; it is not accessible from the Internet, it requires second factor authentication or is access limited to a specific address.

**The organisation has checked and verified that firewall rules ensure that all unauthenticated inbound connections are blocked by default.**

All inbound firewall rules (other than default deny) are documented with business justification and approval by the change management process.

Firewall rulesets are reviewed on a regular basis. Rulesets are removed/disabled when they are no longer required.

All of your organisation’s desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by default.

### Control Objective

The organisation's firewalls block unauthenticated inbound connections by default to prevent unauthorised, and potentially malicious, network connections from being made.

### Approach

1. Review the organisation's firewall configurations and confirm that they are configured to block all unauthenticated inbound connections by default.

### Assessment Documentation

1. Firewall configurations.
2. Security assessment results (e.g. Onsite Assessment)

# Standard 9: Assertion 6

## Evidence Item 9.6.4

The organisation is protected by a well managed firewall.

**Mandatory**

| Category |
| --- |
| 2 |

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

One or more firewalls (or similar network device) have been installed on all the boundaries of the organisation's internal network(s).

The administrative interface used to manage the boundary firewall has been configured such that; it is not accessible from the Internet, it requires second factor authentication or is access limited to a specific address.

The organisation has checked and verified that firewall rules ensure that all unauthenticated inbound connections are blocked by default.

**All inbound firewall rules (other than default deny) are documented with business justification and approval by the change management process.**

Firewall rulesets are reviewed on a regular basis. Rulesets are removed/disabled when they are no longer required.

All of your organisation’s desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by default.

### Control Objective

Changes to firewall rulesets are restricted to prevent unauthorised, and potentially malicious, network connections from being made. Inbound firewall rules are subjected to appropriate governance and change management control / approval processes.

### Approach

1. Determine if the organisation has a documented process that outlines how changes to firewall rulesets should be managed. If such a process exists, review it and determine if it mandates segregation of duties between the reviewer and approver. Only a small number of authorised individuals should have the capability to authorise firewall ruleset changes.

2. For a sample of firewall ruleset changes, review evidence that it was approved by one of the authorised individuals.

### Assessment Documentation

1. Change management policy/procedure that includes firewall ruleset changes in scope.

2. Evidence associated with the approval of a sample of firewall ruleset changes.

Back

# Standard 9: Assertion 6

## Evidence Item 9.6.5

The organisation is protected by a well managed firewall.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

One or more firewalls (or similar network device) have been installed on all the boundaries of the organisation's internal network(s).

The administrative interface used to manage the boundary firewall has been configured such that; it is not accessible from the Internet, it requires second factor authentication or is access limited to a specific address.

The organisation has checked and verified that firewall rules ensure that all unauthenticated inbound connections are blocked by default.

All inbound firewall rules (other than default deny) are documented with business justification and approval by the change management process.

**Firewall rulesets are reviewed on a regular basis. Rulesets are removed/disabled when they are no longer required.**

All of your organisation’s desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by default.

### Control Objective

Firewall rulesets are reviewed on a regular basis. Rulesets are removed/disabled when they are no longer required.

### Approach

1. Determine if the organisation reviews its firewall rulesets on a regular basis. Review evidence associated with the previous three firewall ruleset reviews, including the rulesets that are removed/disabled.

### Assessment Documentation

1. Evidence associated with previous firewall ruleset reviews, including the rulesets that are removed/disabled.

Back

# Standard 9: Assertion 6

## Evidence Item 9.6.6

The organisation is protected by a well managed firewall.

**Mandatory**

| Category |
| --- |
| 2 |

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

One or more firewalls (or similar network device) have been installed on all the boundaries of the organisation's internal network(s).

The administrative interface used to manage the boundary firewall has been configured such that; it is not accessible from the Internet, it requires second factor authentication or is access limited to a specific address.

The organisation has checked and verified that firewall rules ensure that all unauthenticated inbound connections are blocked by default.

All inbound firewall rules (other than default deny) are documented with business justification and approval by the change management process.

Firewall rulesets are reviewed on a regular basis. Rulesets are removed/disabled when they are no longer required.

**All of your organisation’s desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by default.**

### Control Objective

Personal firewalls (on laptops / individual end user devices) are enabled and configured to prevent an individual endpoint from making a potentially malicious network connection.

### Approach

1. Determine if the organisation has personal firewalls in place and review evidence of the control implementation, such as reporting from the administrative console, or alerts when the firewall rulesets are triggered.

2. Spot check the personal firewall ruleset configurations and confirm that they are designed to block unapproved connections by default.

### Assessment Documentation

1. Evidence associated with implementation of personal firewalls.

2. Personal firewall configurations.

# Standard 10 - Accountable Suppliers

The NHS Big Picture Guidance

IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

IT suppliers understand their obligations as data processors under the GDPR, and the necessity to educate and inform customers, working with them to combine security and usability in systems. IT suppliers typically service large numbers of similar organisations and as such represent a large proportion of the overall 'attack surface'. Consequently, their duty to robust risk management is vital and should be built into contracts as a matter of course. It is incumbent on suppliers of all IT systems to ensure their software runs on supported operating systems and is compatible with supported internet browsers and plugins.

**Typical departments responsible for this standard:** Procurement, supplier management, Data Security and Protection

## Overview of standard

### Assertion 1

The organisation can name its suppliers, the products and services they deliver and the contract durations.

### Assertion 2

Basic due diligence has been undertaken against each supplier that handles personal information

### Assertion 3

All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented.

# Standard 10: Assertion 1

The organisation can name its suppliers, the products and services they deliver and the contract durations.

## Objective

Having a centralised list of all suppliers, enables an organisation to identify suppliers that could potentially pose a data security or data protection risk to the organisation. Contracts with these suppliers should have data protection-related clauses, including the responsibilities for the data (e.g. Controller - Processor).

**Category 2**

Back

# Standard 10: Assertion 1

## Evidence Item 10.1.1

The organisation can name its suppliers, the products and services they deliver and the contract durations.

Mandatory

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

The organisation has an up to date list of its suppliers, which enables it to identify suppliers that could potentially pose a data security or data protection risk to the organisation. The list includes which suppliers process personal data or provide IT services on which critical services rely, details on the product and services they deliver, contact details and contract duration.

Contracts with all third parties that handle personal information are compliant with ICO guidance.

### Control Objective

The organisation has a centralised list of all suppliers, which enables it to identify suppliers that could potentially pose a data security or data protection risk to the organisation.

### Approach

1. Determine if the organisation has a centralised list of all suppliers, and assess the process to update it on a regular basis to ensure it accurately reflects the organisation's supplier landscape.

2. Request the supplier list and confirm that it includes; which suppliers process personal data or provide IT services on which critical services rely, details on the products and services they deliver, contact details and the contract duration.

### Assessment Documentation

1. Supplier management policy/process.

2. Supplier list.

# Standard 10: Assertion 1

## Evidence Item 10.1.2

The organisation can name its suppliers, the products and services they deliver and the contract durations.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

The organisation has an up to date list of its suppliers, which enables it to identify suppliers that could potentially pose a data security or data protection risk to the organisation. The list includes which suppliers process personal data or provide IT services on which critical services rely, details on the product and services they deliver, contact details and contract duration.

Contracts with all third parties that handle personal information are compliant with ICO guidance.

### Control Objective

The organisation has updated its supplier contracts to ensure that they are aligned to the requirements of the GDPR.

### Approach

1. Understand if the organisation has updated its supplier model contract to include data privacy terms aligned to Article 28 of the GDPR.

2. Determine if the organisation reviews its supplier contracts on a periodic basis to identify any contracts that do not contain the updated data privacy clauses.

3. Review a sample of contracts with suppliers that process personal data and identify if the updated model clauses have been included.

### Assessment Documentation

1. Documented roles and responsibilities for the accountable individual. These should make explicit reference to data security and protection.

Back

# Standard 10: Assertion 2

Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS England guidance.

## Objective

In order to protect against data security and protection risks in the supply chain, organisations should take a risk-based approach to seeking assurance over the effectiveness of their suppliers' data security and protection control environments.

**Category 1**

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 10: Assertion 2

## Evidence Item 10.2.1

Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS England guidance.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation ensures that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.

Percentage of suppliers with data security contract clauses in place.

Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility.

All suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.

### Control Objective

The organisation confirms that the supplier has the appropriate information security accreditations/certifications, prior to signing the contract. The NHS Improvement 2017/18 Data Security Protection Requirements: guidance states that these could include; ISO 27001:2013, Cyber Essentials, Cyber Essentials Plus, or meets the Digital Marketplace requirements.

### Approach

1. Determine if the organisation has formally documented the accreditations/certifications it requires of suppliers that provide health and social care services, or suppliers that have access to the organisation's data. Determine if there is a process in place to help ensure these accreditations are obtained and verified prior to signing the contract. Review this document and assess whether the requirements are appropriate. For example, Cyber Essentials may not be sufficient for a supplier with whom a large volume of sensitive patient data is shared and further assurances over and above Cyber Essentials are likely to be requested / sought.

2. For a sample of in-scope suppliers, review evidence that the accreditations/certifications were sought prior to on-boarding, and are requested on at least an annual basis.

### Assessment Documentation

1. Supplier requirements document.

2. Sample of supplier accreditations/certifications, including detail on their scope.

3. Where ISO 270001 is in place, check the scope statement on the certificate and the statement of applicability.

# Standard 10: Assertion 2

## Evidence Item 10.2.3

Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS England guidance.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation ensures that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.

**Percentage of suppliers with data security contract clauses in place.**

Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility.

All suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.

### Control Objective

The organisation has updated its supplier contracts to include data security and protection clauses/requirements.

### Approach

1. Understand if the organisation has updated its supplier model contract to include data security and protection clauses/requirements. These could include details on the controls that the supplier should implement (e.g. encryption of data at rest / encryption of data in transit) to protect the organisation's data.

2. Determine if the organisation reviews its supplier contracts on a periodic basis to identify any contracts that do not contain the updated data security and protection clauses/requirements and to assess the currency and fitness for purpose of the contract given the changing nature of the risk, threat and possibly hosting environment (e.g. use of cloud).

3. Review a sample of contracts with suppliers that process personal data and identify if the updated model clauses have been included.

### Assessment Documentation

1. Supplier model contract.

2. Sample of contracts with suppliers that process personal data.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 10: Assertion 2

## Evidence Item 10.2.4

Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS England guidance.

**Mandatory**

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation ensures that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.

Percentage of suppliers with data security contract clauses in place.

**Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility.**

All suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.

### Control Objective

1. The organisation understands that outsourcing technology services does not necessarily result in the transferring of risk, and therefore formally documents the roles and responsibilities of both parties where technology services are outsourced - to achieve clarity as regards accountability for data security and data protection risks.

### Approach

1. Review the organisation's IT procurement policy (or similar) and determine if there is a requirement to document the roles and responsibilities for both parties under the relationship, particularly for technical security controls, such as to what level the supplier has responsibility for patch management.

2. Review a sample of outsourced supplier contracts and determine if the responsibilities of both parties are included.

### Assessment Documentation

1. Roles and responsibilities/RACI matrix for a sample of outsource suppliers.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 10: Assertion 2

## Evidence Item 10.2.5

Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS England guidance.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Your organisation ensures that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.

Percentage of suppliers with data security contract clauses in place.

Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility.

**All suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.**

### Control Objective

The organisation seeks assurances that all of its suppliers that process or have access to health care or personal confidential information have completed the Data Security and Protection Toolkit, or equivalent.

### Approach

1. Review the organisation's supplier list and confirm that it includes detail on which suppliers process or have access to health or care personal confidential information or access to the network / IT infrastructure.

2. Confirm there is a process by which Management seeks assurance that the relevant suppliers have completed the Data Security and Protection Toolkit. Review evidence associated with this for a sample of in-scope suppliers, and confirm whether Management has requested their submission to identify any additional supplier security risks.

3. Select a sample of the organisation's relevant suppliers and confirm that they have completed a DSP Toolkit response via https://www.dsptoolkit.nhs.uk/OrganisationSearch.

### Assessment Documentation

1. Supplier list, containing details on those suppliers that process or have access to health or care personal confidential information.

2. Evidence or procedural documentation that Management seeks assurance that the in-scope suppliers have completed their DSP Toolkit submission.

Back

# Standard 10: Assertion 3

All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented.

## Objective

It is important, in order to effectively manage data security and protection incidents, that communication and engagement with suppliers is included in an organisation's response plan. This is particularly important for incidents that may have been caused by the supplier.

**Category 2**

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# Standard 10: Assertion 3

## Evidence Item 10.3.1

All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented.

**Category**

2

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

List of data security incidents – past or present – with current suppliers who handle personal information.

### Control Objective

The organisation has processes in place to effectively manage, and learn from, previous cyber security incidents that were either caused by its suppliers or were as a result, in part of in full, of weaknesses in the supply chain.

### Approach

1. Review the organisation's cyber security and protection incident response plan/policy/process and confirm that it includes a mechanism for interacting with suppliers during an incident; both in terms of being notified by an incident from a supplier, and engaging with the supplier through to resolution and beyond to lessons learned and continuous improvement activities.

2. Review documentation associated with any such incidents and confirm that they were managed in line with the plan/policy/process.

### Assessment Documentation

1. Data security and protection incident response plan/policy/process.

2. Sample of incident documentation.

NHS England

Introduction

Standards

Standard 1

Standard 2

Standard 3

Standard 4

Standard 5

Standard 6

Standard 7

Standard 8

Standard 9

Standard 10

# NHS England Security and Protection Toolkit Independent Assessment Framework

Information and technology
for better health and care