NHS
Improvement

2017/18 Data Security Protection Requirements: guidance

April 2018

Background

In January 2018, to improve data security and protection for health and care organisations the Department of Health and Social Care, NHS England and NHS Improvement published a set of 10 data and cyber security standards – the 17/18 Data Security Protection Requirements (2017/18 DSPR) – that all providers of health and care must comply with.

The 2017/18 DSPR standards are based on those recommended by Dame Fiona Caldicott, the National Data Guardian (NDG) for health and care, and confirmed by government in July 2017.

We are asking all providers to confirm to us whether or not you are complying with the 2017/18 DSPR standards. To do this, you must submit a response using the web form.

The questions set out below are the same as those found in the web form. They are designed to test whether you have implemented (fully, partially or not) the 10 standards outlined in the 2017/18 DSPR.

As part of the assurance process, the board must sign off your response before it is submitted.

Any questions about the data collection process should be directed to nhsi.17-18dsprsubmission@nhs.net

Leadership obligation 1: People

1. Senior level responsibility

There must be a named senior executive responsible for data and cyber security in your organisation.

Ideally this person will also be your senior information risk owner (SIRO), and where applicable a member of your organisation's board.

Fully implemented	Partially implemented	Not implemented
The organisation has a named senior executive who reports to the board who is responsible for data and cyber security and this person is also the SIRO	The organisation has a named senior executive who reports to the board who is responsible for data and cyber security but this person is not the SIRO	The organisation does not have a named senior executive who is responsible for data and cyber security

Please provide the contact details of the named senior executive responsible for data and cyber security if they are in place.

Name	
Job title	
Name of organisation	
Email	
Telephone number	

2. Completing the Information Governance toolkit v14.1

By 31 March 2018 organisations are required to achieve at least level 2 on the Information Governance (IG) toolkit. More information about the IG toolkit v14.1 can be found here: www.igt.hscic.gov.uk/help.aspx

For more information on how to complete the toolkit, please refer to the guidance:

- NHS foundation trusts: acute trusts, mental health trusts, ambulance trusts, community health providers, commissioning support units, NHS England

- independent providers: nhs business partners, commercial third parties, secondary use organisations, hosted secondary use teams, any qualified providers – clinical and any qualified providers – non clinical.

NOTE: the new Data Security and Protection toolkit is being introduced for 2018/19. This will replace the current IG toolkit.

Fully implemented	Partially implemented	Not implemented
The organisation has completed the IG toolkit, submitted its results to NHS Digital and obtained either level 2 or 3.	The organisation has completed the IG toolkit and submitted its results to NHS Digital but has not attained level 2.	The organisation has not completed the IG toolkit and submitted the results to NHS Digital

3. Preparing for the introduction of the General Data Protection Regulation in May 2018

The beta version of the Data Security and Protection toolkit was released in February 2018 and will help organisations understand what actions they need to take to implement the General Data Protection Regulation (GDPR) which comes into effect in May 2018.

Detailed information about the implementation of the GDPR can be found in the implementation checklist produced by the Information Governance Alliance (https://digital.nhs.uk/information-governance- alliance/General-Data-Protection-Regulation-guidance)

Fully Implemented	Partially Implemented	Not Implemented
By May 2018, the organisation will have an approved plan to detail how it will achieve compliance with the GDPR. This will have board-level sponsorship and approval.	By May 2018, the organisation will have a plan that has been developed but not yet sponsored and approved at board level on how it will achieve compliance with the GDPR.	A plan has not been yet been developed.

4. Training staff

All staff must complete appropriate annual data security and protection training.

As per the IG toolkit, staff are defined as: all staff, including new starters, locums, temporary, students and staff contracted to work in the organisation.

A new training programme has been introduced: https://www.e-lfh.org.uk/programmes/data-security-awareness/. This programme replaces the previous IG training whilst retaining key elements of it. More information about the previous IG training resources can be found at https://www.igt.hscic.gov.uk/NewsArticle.aspx?tk=431663506918390&lnv=1&cb=6fa0a573-a4df-45f3-8af1-5c5ff58cce87&artid=170&web=yes

Providers must ensure staff have completed either the new IG training tool or the previous IG training tool.

Fully implemented	Partially implemented	Not implemented
At least 95% of staff have completed either the previous IG training or the new training in the last twelve months.	At least 85% of staff have completed either the previous IG training or the new training in the last twelve months.	Less than 85% of staff have completed either the previous IG training or the new training

Leadership Obligation 2: Processes

5. Acting on CareCERT advisories

Organisations must:

- Identify a primary point of contact for your organisation to receive and co-ordinate your organisation's response to CareCERT advisories, and provide this information through CareCERT Collect
- act on CareCERT advisories where relevant to your organisation
- confirm within 48 hours that plans are in place to act on High Severity CareCERT advisories, and evidence this through CareCERT Collect

Fully implemented	Not implemented
The organisation has registered for CareCERT Collect	The organisation has not registered for CareCERT Collect

Yes	No	Not applicable
The organisation has plans in place for all CareCERT advisories up to 31/3/2018 that are applicable to the organization (**Note**: the plan could be that the board accepts the residual risk)	The organisation does not have plans in place for all CareCERT advisories up to 31/3/2018 that are applicable to the organisation	The organisation has not registered for CareCERT Collect

Fully implemented	Partially implemented	Not implemented
The organisation has clear processes in place that allow it to confirm within 48 hours of a High Severity CareCERT advisory being issued that a plan is in place.	The organisation does not have clear processes in place that allow it to confirm within 48 hours of a High Severity CareCERT advisory being issued that a plan is in place, but is developing these processes	The organisation does not have clear processes in place that allow it to confirm within 48 hours of a High Severity CareCERT advisory being issued that a plan is in place, and these processes are not under development

Fully implemented	Partially implemented	Not implemented
The organisation has in post a primary point of contact who is responsible for receiving and co-ordinating CareCERT advisories.	The organisation does not have in post a primary point of contact who is responsible for receiving and co-ordinating CareCERT advisories, but is in the process of filling that role.	The organisation does not have in post a primary point of contact who is responsible for receiving and co-ordinating CareCERT advisories, and no plans are in place to fill that role.

6. Business continuity planning

Comprehensive business continuity plans must be in place to support the organisation’s response to data and cyber security incidents.

Fully implemented	Partially implemented	Not implemented
The organisation has an agreed business continuity plan(s) for cyber security incidents in place. The plan(s) take into account the potential impact of any loss of services on external organisations in the health and care system.	The organisation is developing a business continuity plan(s) for data and cyber security incidents. The plan(s) will take into account the potential impact of any loss of services on external organisations in the health and care system.	The organisation does not have a continuity plan for data and cyber security incidents in place

If there is a business continuity plan in place has it been tested in 2017/18?

Yes	No
The business continuity plan for cyber security incidents in has been tested in 2017/18.	The business continuity plan for data and cyber security incidents has not been tested in 2017/18.

7. Reporting incidents

Staff across the organisation must report data security incidents and near misses, and incidents should be reported to CareCERT in line with reporting guidelines.

Incidents should be reported to CareCERT via carecert@nhsdigital.nhs.uk or 03003035222 if part of a national cyber incident response.

Fully implemented	Partially implemented	Not implemented
The organisation has a process or working procedure in place for staff to report data security incidents and near misses	The organisation is developing a process or working procedure for staff to report data security incidents and near misses	The organisation does not have a process or working procedure in place for staff to report data security incidents and near misses

Leadership obligation 3: Technology

8. Unsupported systems

Your organisation must:

- identify unsupported systems (including software, hardware and applications)
- have a plan in place by April 2018 to remove, replace or actively mitigate or manage the risks associated with unsupported systems.

NHS Digital’s good practice guide on the management of unsupported systems is at: https://digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care.

Other guidance and general documents are on the main CareCERT website.

Fully implemented	Partially implemented	Not implemented
The organisation has reviewed all its systems and any unsupported systems have been identified and logged on the organisation’s relevant risk register	The organisation has reviewed all its systems and any unsupported systems have been identified but not logged on the organisation’s relevant risk register	The organisation has not reviewed its systems to identify any that are unsupported

For any unsupported systems identified, has the organisation developed a plan for how it will remove, replace or actively mitigate or manage the risks of unsupported systems. Organisations are not required to submit a plan as part of this data collection process but should be prepared to submit their plan to NHS Digital if requested.

Fully implemented	Not implemented
By May 2018 the organisation will have developed a plan to remove, replace or actively mitigate or manage the risks associated with unsupported systems	By May 2018 the organisation will not have a plan in place to remove, replace or actively mitigate or manage the risks associated with unsupported systems

9. On-site cyber and data security assessments

Your organisation must:

- have undertaken or have signed up to an on-site cyber and data security assessment by NHS Digital
- act on the outcome of that assessment, including any recommendations, and share the outcome of the assessment with your commissioner.

Fully implemented	Partially implemented	Not implemented
The organisation has undergone an NHS Digital on-site cyber and data security assessment	Prior to 31 March 2018 the organisation signed up to undergo an NHS Digital on-site cyber and data security assessment but has not yet	Prior to 30 March 2018 the organisation has not signed up to an NHS Digital on-site cyber and data security assessment

For organisations who have undergone an NHS Digital on-site cyber and data security assessment:

Fully implemented	Partially implemented	Not implemented
The organisation has an improvement plan in place on the basis of the findings of the assessment, and has shared the outcome with the relevant commissioner(s)	The organisation has an improvement plan in place on the basis of the findings of the assessment, but has not yet shared the outcome with the relevant commissioner(s)	The organisation does not yet have an improvement plan in place on the basis of the findings of the assessment, and has not yet shared the outcome with the relevant commissioner(s)

Please tell us if the organisation has used an external organisation to audit the organisation’s data and cyber security risks. Please note there is no requirement to use an external organisation to audit data and cybersecurity risks.

Yes	No
The organisation has used an external vendor to audit the organisation’s data and cyber security risks	The organisation has not used an external vendor to audit the organisation’s data and cyber security risks

10. Checking Supplier Certification

Organisation should ensure that any supplier of critical IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification (suppliers may include other health and care organisations).

Depending on the nature and criticality of the service provided, certification might include:

- ISO/IEC 27001:2013 certification: supplier holds a current ISO/IEC27001:2013 certificate issued by a United Kingdom Accreditation Service (UKAS)-accredited certifying body and scoped to include all core activities required to support delivery of services to the organisation.

- Cyber Essentials (CE) certification: supplier holds a current CE certificate from an accredited CE certification body.

- Cyber Essentials Plus (CE+) certification: supplier holds a current CE+ certificate from an accredited CE+ Certification Body.

- Digital Marketplace: supplier services are available through the UK Government Digital Marketplace under a current framework agreement.

- Other types of certification may also be applicable. Please refer to Cyber Security Services 2 Framework via Crown Commercial (https://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3764ii)

NHS Digital contracts for/supplies a number of IT systems and solutions in use by multiple NHS organisations. Please note that NHS Digital ensures in each of its system procurements that appropriate data security certifications are in place from its suppliers.

Fully implemented	Partially implemented	Not implemented
The organisation has checked that the suppliers of all its IT systems have appropriate certification, and can evidence that all suppliers have such certification.	The organisation has checked that the suppliers of IT systems that relate to patient data, involve clinical care or identifiable data have appropriate certification, and can evidence that all suppliers have such certification.	The organisation has not checked whether its suppliers of IT systems have appropriate certification.

0300 123 2257 **enquiries@improvement.nhs.uk** **improvement.nhs.uk**