Department of Health

NHS England

2017/18 Data Security and Protection Requirements

October 2017

Title: 2017/18 Data Security and Protection Requirements
Author: DDP / 13920
Document Purpose: Guidance
Publication date: October 2017
Target audience: NHS Providers General Practice Social Care
Contact details: Digital, Data and Primary Care Department of Health Quarry House, Leeds / 39 Victoria Street, London

You may re-use the text of this document (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit www.nationalarchives.gov.uk/doc/open-government-licence/

© Crown copyright

Published to gov.uk, in PDF format only.

www.gov.uk/dh

2017/18 Data Security and Protection Requirements

Department of Health

NHS England

NHS Improvement

Summary

This document sets out the steps all health and care organisations will be expected to take in 2017/18 to demonstrate that they are implementing the ten data security standards recommended by the National Data Guardian, and further details regarding the assurance framework for April 2018 onwards.

Background

On 12 July 2017 the Government accepted the ten data security standards recommended by Dame Fiona Caldicott, the National Data Guardian for Health and Care.

https://www.gov.uk/government/news/national-data-guardian-ndg-statement-on-government-response-to-the-ndg-review

This document sets out the steps all health and care organisations will be expected to take in 2017/18 to demonstrate that they are implementing the ten data security standards, prior to a new assurance framework coming into place from April 2018.

From April 2018 the new Data Security and Protection Toolkit (DSP Toolkit) replaces the Information Governance Toolkit (IG Toolkit). It will form part of a new framework for assuring that organisations are implementing the ten data security standards and meeting their statutory obligations on data protection and data security. Further information on the new assurance framework, which will build on these requirements, is provided in this document.

Who these requirements apply to

Both the ten data security standards, and the 2017/18 requirements, apply to **all** health and care organisations. When considering data security as part of the 'well led' element of their inspections, the Care Quality Commission will look at how organisations are assuring themselves that the steps set out in this document are being taken.

More information on the Care Quality Commission inspection frameworks can be found here: http://www.cqc.org.uk/guidance-providers

NHS providers

Organisations contracted to provide services under the NHS Standard Contract (NHS providers) must comply with the requirements set out in this document, as part of the data security and protection requirements set out in that contract. At the end of the 2017/18 financial year NHS Improvement will ask NHS providers to confirm that they have implemented the requirements set out in this document. In the longer term NHS Improvement will ensure that data security is included in their oversight arrangements.

General Practice

General Practices, contracted to provide primary care essential services to a registered list under the NHS standard General Medical Services (GMS) contract (or Personal Medical Services (PMS) or Alternative Provider Medical Services (APMS) contracts), must comply with the requirements set out in this document, as part of the data security and protection requirements set out in that contract. Some requirements will be implemented by the commissioner of the GP IT & GP Information Governance Support Service (Clinical Commissioning Group (CCG) or NHS England Regional) on their behalf.

Social Care

For social care providers, who do not provide NHS care through the NHS Standard Contract, there are no obligations to implement the requirements set out in this document in this financial year. However, it is highly recommended that social care organisations follow these steps in preparation for the new regulatory framework from April 2018 onwards.

Part A: 2017/18 Data Security Requirements

This section sets out the steps that all health and care organisations are required to take in 2017/18 to implement the data security standards. These requirements are across the three leadership obligations under which the data security standards are grouped: people, process and technology. (Part B sets out how these requirements apply to general practice.)

Leadership Obligation One – People:

1. **Senior Level Responsibility**: There must be a named senior executive to be 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.
2. **Completing the Information Governance Toolkit v14.1**: In 2017/18, organisations are still required to achieve at least level two on the current IG Toolkit before it is replaced with a new approach (the new Data Security and Protection Toolkit), from 2018/19 onwards, to measuring progress against the 10 data security standards.
3. **Complete the General Data Protection Regulation Checklist**: NHS Digital will publish a checklist to support organisations in implementing the requirements of the General Data Protection Regulation which they will be required to comply with from May 2018. Organisations must complete this checklist to ensure they will be able to meet their legal obligations from May 2018.
4. **Training Staff**: All staff must complete appropriate annual data security and protection training. This training replaces the previous Information Governance training while retaining key elements of it. It contains new sections on cyber security. https://www.e-lfh.org.uk/programmes/data-security-awareness/

Leadership Obligation Two - Processes:

5. **Acting on CareCERT advisories**: Organisations must:
    - 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; and
    - Identify a primary point of contact for your organisation to receive and coordinate your organisation's response to CareCERT advisories, and provide this information through CareCERT Collect.

Note: Action might include understanding that an advisory is not relevant to your organisation's systems and confirming that this is the case.

More information on CareCERT (including CareCERT Collect) can be found here: https://nww.carecertisp.digital.nhs.uk/

Organisations wishing to sign up or log in to CareCert Collect should go to https://nww.carecertcollect.digital.nhs.uk

6. **Continuity planning**: A comprehensive business continuity plan must be in place to respond to data and cyber security incidents.
7. **Reporting incidents**: Staff across the organisation report data security incidents and near misses, and incidents are reported to CareCERT in line with reporting guidelines.

Leadership Obligation Three - Technology:

8. **Unsupported systems**: Your organisation must:
    - Identify unsupported systems (including software, hardware and applications); and
    - Have a plan in place by April 2018 to remove, replace or actively mitigate or manage the risks associated with unsupported systems.

    NHS Digital good practice guidance on the management of unsupported systems can be found here: https://www.digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care/legacy-hardware-software-unsupported-platforms/good-practice-guide

9. **On-Site Assessments**: Your organisation must:
    - Undertake an on-site cyber and data security assessment if you are invited to do so by NHS Digital; and
    - Act on the outcome of that assessment, including any recommendations, and share the outcome of the assessment with your commissioner.
10. **Checking Supplier Certification**: Your organisation should ensure that any supplier of IT systems (including other heath and care organisations) and the system(s) provided have the appropriate certification. A list of certification frameworks is provided below.

Supplier Certification Frameworks

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 UKAS accredited certifying body and scoped to include all core activities required to support delivery of services to the organisation.
- *Cyber Essentials (CE) certification* - The supplier holds a current CE certificate from an accredited CE Certification Body.
- *Cyber Essentials Plus (CE+) certification* - The 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

It should be noted that where a provider holds certification it is not always the case that the services they provide are certified to the same level. Further, placement on a procurement

framework does not guarantee the level of certification of a supplier or service. In general, Cyber Essentials should be considered a minimum requirement.

Part B: 2017/18 Data Security Requirements – General Practices

This section sets out the steps that General Practitioners are required to take in 2017/18 to implement the data security standards. These requirements are across the three leadership obligations under which the data security standards are grouped: people, process and technology.

Leadership Obligation One – People:

1. **Senior Level Responsibility**: Each practice must have a named partner, board member or equivalent senior employee to be responsible for data and cyber security in the practice. The CCG as commissioner will be responsible for providing specialist support to this role but each practice remains accountable.
2. **Completing the Information Governance Toolkit v14.1**: Each practice remains accountable and responsible for completing the current GP IG Toolkit with a recommendation that practices attain level two as a minimum. From 2018/19 onwards it will be replaced with a new approach to measure progress against the 10 data security standards. The commissioned GP IG services are available to support practices in this. The locally commissioned GP IT Delivery partner will also be contractually required to complete the current IG toolkit to at least level two for their organisation and the services delivered under the GP IT contract.
3. **Complete the General Data Protection Regulation Checklist**: NHS Digital will publish a checklist to support public authority organisations (including general practices) in implementing the requirements of the General Data Protection Regulation which they will be required to comply with from May 2018. General Practices should complete this checklist to ensure they will be able to meet their legal obligations from May 2018. Each general practice will be accountable and responsible for completing this, including the appointment of a Data Protection Officer (DPO). The commissioned GP IT & Information Governance services will support practices through a DPO Support function.
4. **Training Staff**: Each general practice is accountable for ensuring all staff complete appropriate annual data security and protection training. Online training is available. This training replaces the previous Information Governance training while retaining key elements of it and adding a new section on cyber security. https://www.e-lfh.org.uk/programmes/data-security-awareness/

General Practice: Each general practice is accountable for this requirement.

Leadership Obligation Two - Processes:

5. Acting on CareCERT advisories: CCGs will ensure the commissioned GP IT delivery partner(s) will be responsible for meeting the following requirements with the CCG holding accountability actioned through exception reporting. Organisations must:
    - Act on CareCERT advisories where relevant to the service provided;
    - Confirm within 48 hours that plans are in place to act on *High Severity* CareCERT advisories and evidence this through CareCERT Collect; and

- Identify a primary point of contact for your organisation to receive and coordinate your organisation's response to CareCERT advisories, and provide this information through CareCERT Collect.

Note: Action might include understanding that an advisory is not relevant to your organisation's systems and confirming that this is the case.

More information on CareCERT (including CareCERT Collect) can be found here: https://nww.carecertisp.digital.nhs.uk/

Organisations wishing to sign up or log in to CareCert Collect should go to https://nww.carecertcollect.digital.nhs.uk

6. **Continuity planning**: Each General Practice is required to continue to maintain a business continuity plan (under IGT requirements and CCG-Practice Agreements) which will include the response to data and cyber security incidents.

   CCGs are required to ensure commissioned GP IT delivery partner(s) will maintain business continuity and disaster recovery plans for services provided to General Practices, which will include responses to data and cyber security incidents.

   Reporting incidents: Each general practice is accountable for ensuring data security incidents and near misses are reported to CareCert in line with reporting guidelines. Practices will be supported by the commissioned GP IT and GP IG services in the reporting and managing of the incident.

Leadership Obligation Three - Technology:

7. **Unsupported systems**: CCGs must ensure for all supported general practices the following:

   - Identify unsupported systems (including software, hardware and applications); and

   - Have a plan in place by April 2018 to remove, replace or actively mitigate and actively manage the risks associated with, unsupported systems.

   NHS Digital good practice guidance on the management of unsupported systems can be found here: https://www.digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care/legacy-hardware-software-unsupported-platforms/good-practice-guide

8. **On-Site Assessments**: CCGs must ensure the commissioned GP IT delivery partner carries out the following for all supported general practices and GP IT infrastructure. General practices are required to fully support such assessments.

   - Undertake an on-site cyber and data security assessment if you are invited to do so by NHS Digital; and

   - Act on the outcome of that assessment, including any recommendations, and share the outcome of the assessment with your commissioner.

All practices will comply with agreed action plans to meet their responsibilities described in the CCG – Practice Agreement.

Where systems and IT infrastructure process person identifiable data outside the scope of the CCG's commissioned GP IT delivery service or GPSoC, then individual general practices are accountable for assuring all of the above requirements are met.

9. Checking Supplier Certification: All parties who commission or procure IT Systems i.e. individual general practices, CCG, GP IT Delivery Partners and NHS Digital (GPSOC) will ensure that any supplier of IT Services, infrastructure or systems used in general practice have the appropriate certification. CCGs will ensure commissioned GP IT services include access to specialist technical advice for IT procurement.

Supplier Certification Frameworks

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 UKAS accredited certifying body and scoped to include all core activities required to support delivery of services to the organisation.
- *Cyber Essentials (CE) certification* - The supplier holds a current CE certificate from an accredited CE Certification Body.
- *Cyber Essentials Plus (CE+) certification* - The 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

It should be noted that where a provider holds certification it is not always the case that the services they provide are certified to the same level. Further, placement on a procurement framework does not guarantee the level of certification of a supplier or service. In general, Cyber Essentials should be considered a minimum requirement.

Understanding the approach to measuring progress from 2018/19 onwards

The approach to measuring progress in implementing the ten data security standards and compliance with data protection legislation, through the Data Security and Protection Toolkit which will replace the Information Governance Toolkit from April 2018, is being tested with over 500 health and care organisations.

In preparing for 2018/19, you may consider that you need to increase your organisation's understanding of data and cyber security:

- Consider the Ten Steps to Cyber Security https://www.ncsc.gov.uk/guidance/10-steps-cyber-security and how these steps might apply to your organisation to support the implementation of the National Data Guardian's recommended data security standards;
- Refer to NHS Digital's Data Security Good Practice Guides for health specific guidance on how to achieve aspects of the Ten Steps to Cyber Security https://www.digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care.

Key dates:

- *November 2017*: The replacement for the Information Governance Toolkit, the new Data Security and Protection Toolkit will be piloted with users.
- *February 2018*: All organisations will have access to the new Data Security and Protection Toolkit from January 2018 to familiarise themselves with the approach to measuring implementation and compliance and consider how they might apply to their organisation from April 2018.
- *April 2018*: Further guidance will be published to support organisations to use the new Data Security and Protection Toolkit.
- *April 2018*: all organisations will now be required to complete the new Data Security and Protection Toolkit.
- *May 2018*: The EU General Data Protection Regulation, and Security of Network and Information Systems Directive, come into force. This will increase the legislative data security and protection requirements on Health and Care organisations