Department of Health & Social Care

NHS England

2017/18 Data Security and Protection Requirements

January 2018

Title: 2017/18 Data Security and Protection Requirements
Author: DDP 13920
Document Purpose: Guidance
Publication date: January/2018/NHS England Gateway Reference - 07571
Target audience: NHS Providers, Local Authorities, Social Care Providers, General Practices, Clinical Commissioning Groups
Contact details: Digital, Data and Primary Care, Department of Health, Quarry House, Leeds / 39 Victoria Street, London

Published to gov.uk, in PDF format only.

www.gov.uk/dh

2017/18 Data Security and Protection Requirements

Prepared by

Department of Health

NHS England

NHS Improvement

Summary

This document sets out the steps health and care organisations are expected to take in 2017/18 to demonstrate that they are implementing the ten data security standards[1], recommended by Dame Fiona Caldicott, the National Data Guardian for Health and Care and confirmed by Government in July 2017. This document also includes further details regarding the assurance framework for April 2018 onwards.

[1] Review of Data Security, Consent and Opt-Outs - Parliament UK

Background

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.

The ten data security standards 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 (CQC) will look at how organisations are assuring themselves that the steps set out in this document are being taken. More information on the CQC 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.

Clinical Commissioning Groups

Clinical Commissioning Groups (CCGs), as discrete NHS organisations responsible for their corporate IT services, must comply with the requirements set out in this document. As commissioners of GP IT services, CCGs must ensure commissioned GP IT providers are contractually required to comply with these requirements.

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 CCG-Practice Agreement (terms governing the provision and receipt of GPSoC services and GP IT services). 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.

Local Authorities and Social Care Providers

A proportionate response is needed for local authorities and social care providers given the context they work within.

Local Authorities

Local authorities should comply with the requirements in this document where they provide adult social care or public health and other services that are receiving services and data from NHS Digital and / or are involved in data sharing across health and care where they process the personal confidential data of citizens who access health and adult social care services.

Social Care Providers

Social care providers who provide care through the NHS Standard contract need to comply with the new DSP Toolkit from April 2018.

For social care providers who do not provide care through the NHS Standard Contract, there is no action to take during 2017/18. However, it is recommended that all social care providers consider compliance with the new DSP Toolkit from April 2018. This will help to demonstrate compliance with the ten data security standards and prepare for the General Data Protection Regulation (GDPR) which comes into force from May 2018.

Further Queries

If you have any queries and / or would like to be signposted to more resources about the DSP Toolkit or CareCERT, please contact NHS Digital's Data Security Centre which provides services, guidance and support to health and care organisations at: cybersecurity@nhs.net

Part A: 2017/18 Data Security and Protection Requirements - NHS organisations

This section sets out the steps that NHS 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 Practices and Part C sets out how these requirements apply to local authorities and social care providers).

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 DSP Toolkit), from 2018/19 onwards, to measuring progress against the ten data security standards.

3. **Prepare for the introduction of the General Data Protection Regulation (GDPR) in May 2018:** The Beta version of the Data Security and Protection Toolkit, to go live in February 2018, will help organisations understand what actions they will need to take to implement GDPR, which comes into effect in May 2018.

4. **Training Staff:** All staff must complete appropriate annual data security and protection training. This training replaces the previous IG training whilst retaining key elements of it: 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 co-ordinate 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 guide on the management of unsupported systems can be found at: https://digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care (and associated documents on the main CareCERT web site)

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 and Protection Requirements – General Practice

This section sets out the steps that General Practitioners, CCGs and their commissioned GP IT Delivery Partner(s) are required to take in 2017/18 to implement the ten data security standards within General Practice. These requirements are across the three leadership obligations under which the ten 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. This requirement further defines existing practice obligations to identify the person with lead responsibility for IT matters in the Practice (CCG-Practice Agreement - 5.3). The CCG as commissioner of GP IT services will be responsible for providing specialist support to this role but each practice remains accountable. CCGs must ensure their commissioned GP IT Delivery Partner has allocated equivalent senior level responsibility for data and cyber security within their organisation.

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 ten 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. **Prepare for the introduction of the General Data Protection Regulation (GDPR) in May 2018:** The Beta version of the Data Security and Protection Toolkit, to go live in February 2018, will help organisations understand what actions they will need to take to implement GDPR, which comes into effect in May 2018.

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 IG training whilst retaining key elements of it: https://www.e-lfh.org.uk/programmes/data-security-awareness/

Leadership Obligation Two - Processes:

5. **Acting on CareCERT advisories:** CCGs will ensure the locally 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:

- 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.

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 at: 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 must continue to maintain a business continuity plan (CCG-Practice Agreement) which will include the response to data and cyber security incidents. CCGs are required to ensure commissioned GP IT delivery partner(s) maintain business continuity and disaster recovery plans for services provided to General Practices, which will include responses to data and cyber security incidents.

7. **Reporting incidents:** Each General Practice is accountable for ensuring data security incidents and near misses are reported to CareCERT in accordance with national reporting guidance and legal requirements (NHS GP IG Toolkit ref 14.1-320). Specialist support for GP Cyber Security incident reporting and management will be part of the commissioned IT security and IG service.

Leadership Obligation Three - Technology:

8. **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 guide on the management of unsupported systems can be found at: https://digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care (and associated documents on the main CareCERT web site)

9. **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 must fully support such assessments, and:

- 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 must 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.

10. **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.

Part C: 2017/18 Data Security and Protection Requirements – Local Government and Social Care Providers

This section sets out the steps that local authorities and social care providers need to take in 2017/18 to implement the ten data security standards. A proportionate response is needed for local authorities and social care providers, given the context they work within.

Local authorities

Local authorities have responsibility for the safe and secure handling of personal and confidential information across a range of services including public health and adult social care. Local authorities may also have access to relevant health information, either to support their care delivery role or to support their commissioning responsibilities.

The ten data security standards will be integrated within the new DSP Toolkit from April 2018. A number of the requirements in the Toolkit will be mandatory for completion (to ensure application of the standards), whilst others will be optional.

As with existing arrangements for the IG Toolkit, non-NHS organisations (including local authorities) will need to complete the new DSP Toolkit where they are accessing systems, services and data provided by NHS Digital or where they provide adult social care or public health.

In addition, the new DSP Toolkit can be used to support the local sharing of health and adult social care information by providing evidence about the effective handling of information across organisations. It may be used by local authorities where they are commissioning or co-commissioning services.

Many local authorities already complete the existing IG Toolkit so this is not a new requirement. The new DSP Toolkit will be relevant for adult social care, public health or other services that may be accessing NHS Digital services or processing health and care information. Many local authorities have used the IG Toolkit across the whole organisation and others may wish to consider this as part of the new Toolkit.

Local authorities already have quality assurance arrangements in place either through the Public Service Network (PSN), ISO or other quality standards. To ensure there is no duplication between these frameworks, the DSP Toolkit will be tailored accordingly where local authorities have completed aspects of the new DSP Toolkit through other quality assurance arrangements. For example, the current PSN IA Certification provides the equivalence to the IG Training Standard in the IG Toolkit and this is planned to continue. Local authorities will therefore only be required to complete the relevant sections. NHS Digital is working closely with the Cabinet Office to ensure these frameworks are aligned to help to reduce any additional requirements from local authorities.

In summary:

- During 2017/18, local authorities should complete the 2017/18 IG Toolkit Version 14.1 where they provide adult social care or public health or are accessing services and data from NHS Digital and / or are involved in data sharing across health and care.

- From April 2018 onwards, local authorities should complete the new DSP Toolkit for adult social care, public health and other services that are receiving services and data from NHS Digital and / or are involved in data sharing across health and care where they process the personal confidential data of citizens who access health and adult social care services.

Social care providers

Social care providers who provide care through the NHS Standard Contract

For social care providers who provide care through the NHS Standard contract, there is a mandatory requirement to comply with the new DSP Toolkit from April 2018.

Social care providers who do not provide care through the NHS Standard Contract

For social care providers who do not provide care through the NHS Standard Contract, there is no action to take during 2017/18.

However, it is recommended that all social care providers consider compliance with the new DSP Toolkit from April 2018 because:

- All social care providers are expected to be compliant with the ten data security standards.
- In preparation for the GDPR which comes into force from May 2018. The GDPR will replace the 1995 data protection directive by bringing together privacy laws across Europe and aims to give greater protection and rights to individuals.

It is acknowledged that few social care providers have completed the existing IG Toolkit. This guidance therefore recognises that many social care providers will need time to enhance their level of digital maturity and develop systems and processes to achieve compliance.

Whilst it will not be mandatory for all social care providers to complete the new DSP Toolkit from 2018/19 and there has been no deadline established for compliance for those who do not operate under the NHS standard contract, the new DSP Toolkit has been designed and tested with social care providers to be both relevant and proportionate to the sector (with accompanying guidance for the sector).

Opportunities for Social Care Providers

The new DSP Toolkit will help social care providers audit their own systems and practices against the ten data security standards, as well as help social care organisations understand how the GDPR will impact on them.

Completing the new DSP Toolkit will also open up opportunities for social care providers to be involved in local information sharing initiatives and gain access to a range of national resources which will support data and cyber security and greater information sharing between health and social care including:

- Access to NHSmail, enabling the sharing of information across organisational and geographical boundaries. This includes the use of collaborative tools such as the NHSmail directory, Skype for Business options and secure email with other NHSmail users and those

who also use secure email systems e.g. local authorities using Microsoft Office 365. NHSmail can be accessed from all common smartphones, tablets and desktop computers.

- Access to Summary Care Records (SCRs) for approved organisations which meet all the necessary IG and data protection requirements. Work has now started to investigate the best secure way for care providers to access SCRs, which traditionally contain key information from General Practitioners including medication, allergies and adverse reactions. Additional information such as details of long-term conditions, significant medical history, personal preferences including specific communications needs can be added with the person's consent. Over 97% of people registered with a General Practice in England (55.2 million people) now have an SCR.

Both options have already been rolled out to Community Pharmacies after completion of the IG Toolkit and much can be learnt from the way they were implemented.

CQC Key Lines of Enquiry (KLOE) include a focus on the use of technology and sharing information for the benefit of the care to the individual. In addition, from 1 November 2017, CQC introduced a new KLOE under the Governance and Management section of the well-led inspection area covering data security. Whilst the KLOE does not specifically reference the DSP Toolkit, it will be looking for providers to operate within a framework that demonstrates robust arrangements around the security, availability, sharing and integrity of confidential data, records and data management standards.

The CQC are piloting using NHS Digital intelligence from the DSP Toolkit, on-site assessments and network monitoring to support them in inspections. Staff learning and training regarding IG in general is key to supporting fulfilment of the KLOE and data security standards.

In summary:

- For social care providers who provide care through the NHS Standard Contract, it will be mandatory to comply with the new DSP Toolkit from April 2018.
- Whilst it will not be mandatory for social care providers who do not provide care through the NHS Standard Contract to complete the new DSP Toolkit from April 2018, it is recommended that providers consider completing it to help demonstrate compliance against the ten data security standards, prepare for the forthcoming GDPR and support information sharing.

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 DSP Toolkit which will replace the IG 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:

- Read 'An Introduction to Cyber Security': http://www.careprovideralliance.org.uk/guidance.html which, although published for social care providers, has information that will be of use to anyone wishing to learn more about 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 ten data security standards.
- Refer to NHS Digital's Data Security Good Practice Guides for health and care - 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 IG Toolkit, the new DSP Toolkit started to be piloted with users.

February 2018: All organisations will have access to the new DSP Toolkit 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 DSP Toolkit.

April 2018: All organisations will now be required to complete the new DSP Toolkit.

May 2018: The EU GDPR, 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.