About the Data Security and Protection Toolkit

Document Management

Revision History

Version	Date	Summary of Changes
0.1	13/12/2017	First draft

Glossary of Terms

Term / Abbreviation	What it stands for
DSP Toolkit	Data Security and Protection Toolkit

Document Control:

The controlled copy of this document is maintained in the Data Security and Protection Toolkit website: www.dsptoolkit.nhs.uk. 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.

Contents

1 Introduction

1.1 What is the Data Security and Protection Toolkit?

The Data Security and Protection (DSP) Toolkit is an online tool that enables organisations to measure their performance against data security and information governance requirements which reflect legal rules and Department of Health policy.

The Toolkit has been developed in response to The NDG Review (Review of Data Security, Consent and Opt-Outs) published in July 2016 and the government response published in July 2017 (see section 3).

The Data Security and Protection Toolkit is the successor framework to the IG Toolkit.

2 Why might you be required to complete an assessment?

2.1 Overview

All organisations that have access to NHS patient information must provide assurances that they are practising good information governance and use the Data Security and Protection Toolkit to evidence this by the publication of annual assessments.

It is also a contractual requirement in the NHS England standard conditions contract[1] (section 21.2) that relevant providers[2] undertake DSP Toolkit assessments on an annual basis: “The Provider must complete and publish an annual information governance assessment and must demonstrate satisfactory compliance as defined in the Information Governance Toolkit (or any successor framework), as applicable to the Services and the Provider’s organisation type.”

It remains Department of Health policy that all bodies that process NHS patient information for whatever purpose should provide assurance via the DSP Toolkit.

Use of the toolkit is also required as part of the DH publication: Data security and protection for health and care organisations October 2017. 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.

2.2 Related legislation, policy and good practice

The standard (and associated guidance) draws together key rules and good practice about how information is handled pertaining to:

[1] https://www.england.nhs.uk/nhs-standard-contract/

[2] Those organisations which are subject to the terms of the NHS England standard contract

- The General Data Protection Regulation.
- The Data Protection Act 1998 (and 2018, currently going through parliament).
- The common law duty of confidentiality.
- The Confidentiality NHS Code of Practice.
- The NHS Care Record Guarantee for England.
- The Social Care Record Guarantee for England.
- The international information security standard: ISO/IEC 27002: 2013 and ISO/IEC 27001: 2013.
- The Information Security NHS Code of Practice.
- The Records Management NHS Code of Practice.
- The Freedom of Information Act 2000.
- The Human Rights Act article 8.
- The 'Report on the review of patient-identifiable information' (alternative title 'The Caldicott Report') and the 'Information: To share or not to share? The Information Governance Review (also known as the Caldicott 2 Review).
- Information: To share or not to share - Government Response to the Caldicott 2.
- National Data Guardian "Review of Data Security Consent and Opt Outs" July 2016
- Government Response "Your Data: Better Security, Better Choice, Better Care" July 2017
- Department of Health "2017/18 Data security and protection for health and care organisations"

3 What is the purpose of the assessment?

The Toolkit provides a mechanism for organisations to demonstrate that they can be trusted to maintain the confidentiality and security of personal information. This in turn increases public confidence that 'the NHS' and its partners can be trusted with personal data. This will minimise the number of individuals who 'opt out' of the sharing of their personal identifiable data.

The toolkit enables organisations to measure their compliance against the law and central guidance and to see whether information is handled correctly and protected from unauthorised access, loss, damage and destruction.

Where partial or non-compliance is revealed, organisations must take appropriate measures, (e.g. assign responsibility, put in place policies, procedures, processes and guidance for staff), with the aim of making cultural changes and raising information governance standards through year on year improvements.

By assessing itself against the standard, and implementing actions to address shortcomings identified though use of the toolkit, organisations will be able to reduce the risk of a data breach.

4 When must assessments be completed?

4.1 First-time assessments

Organisations carrying out their first assessment should complete this in line with the contract of services they are party to, or as required by the tendering process they are involved in.

Where a first assessment is being carried out as part of an application for national systems and services, the organisation should complete this as soon as they are able as connection will not be granted until an assessment has been published and reviewed by NHS Digital.

Similarly, for Research Teams or National Registers required to complete a DSP Toolkit assessment in support of an application to access patient information held on national systems, held by NHS Digital or required for processing without consent (for both research and non-research purposes). The DSP Toolkit assessment should be completed within given timelines determined by the approval processes concerned (e.g. section 251 approvals by the Health Research Authority Confidentiality Advisory Group).

4.2 Second assessments

A second or subsequent assessment can be started at any time but in all cases the final publication must be made online by 31 March each year.

Larger NHS organisations are also required to complete interim assessments during the year - deadlines for interim submission will be [TBC]. This will be publicised by writing to all the organisations covered by the scope of the interim assessments and communication through the Strategic Information Governance Network.

The work necessary to make improvements or to maintain compliance should be an on-going process and not left till the year end.

Final publication assessment scores reported by organisations are used by the Care Quality Commission for use as part of the Well Led inspection.