Data Security and Protection Policy

Data Security and Protection Policy

Contents

Document History

Document Reference:	…
Document Purpose:	This policy sets out the Riverside Surgery framework for maintaining and enhancing a high-quality data such as complete, accurate, appropriate, accessible and timely data in all forms.
Date Approved:	4 January 2023
Version Number:	5.0
Status:	FINAL
Next Revision Due:	January 2024
Reviewed by	Data Business Analyst
Policy Sponsor:	Business Manager
Target Audience:	This policy applies to any person directly employed, contracted, working on behalf of the Practice or volunteering with the Practice.
Associated Documents:	All Information Governance Policies and the Information Governance Toolkit, and Data Security and Protections Toolkit 2022/23

Introduction

Guidance statement

The NHS Digital Data Security and Protection Toolkit (DSPT) is a replacement for the Information Governance Toolkit and was introduced in April 2018. The Surgery is required to provide assurance that they have good data security processes in place and patient information is managed appropriately.

Principles

This document will illustrate the practice's commitment to the safety of patient information. By adhering to the referenced guidance, staff will ensure that data and information are protected, which will reduce the risk of information security incidents in the future.

Status

The practice aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over

others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have in regard to the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment.

Training and support

The practice will provide guidance and support to help those to whom it applies understand their rights and responsibilities under this guidance. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this guidance.

Scope

Who it applies to

This document applies to all employees, partners, and directors of the practice. Other individuals performing functions in relation to the practice, such as agency workers, locums and contractors, are encouraged to use it.

Why and how it applies to them

It is the responsibility of all staff to ensure that they handle patient information and data in the appropriate manner, and in accordance with the data security standards.

Definition of terms

Data Security and Protection Toolkit

The Data Security and Protection Toolkit (DSPT) is an online self-assessment tool which allows practices to measure their performance against the National Data Guardian's ten data security standards.

Requirements

Rationale

The DSPT has been designed to support the requirements of the General Data Protection Regulation (GDPR) and the National Data Guardian's (NDG) ten data security standards.

The Surgery is required to complete an annual assessment to provide assurance that data security is of a good standard and patient information and data are handled in line with the data security standards. Assessments are to be submitted by 31 March annually.

NDG expectations

The NDG is Dame Fiona Caldicott and the requirements of the NDG are:

- 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.
- All staff understand their responsibilities under the NDG Data Security Standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
- All staff complete appropriate annual data security training and pass a mandatory test.

Data Security Standards

The ten standards

The purpose of the standards is to enhance existing data security principles, thereby improving data security across the healthcare sector. The standards outline the value of safe, secure, appropriate and lawful sharing of data.

The Data Security Standards are:

- All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful and appropriate purposes.
- 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 complete appropriate annual data security training and pass a mandatory test, provided through Teamnet Training.
- 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 instances of access to personal confidential data on IT systems can be attributed to individuals.
- Processes are reviewed at least annually to identify and improve any which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
- 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.

- 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.
- No unsupported operating systems, software or internet browsers are used within the IT estate.
- A strategy is in place for protecting IT systems from cyber threats, based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
- IT suppliers are held accountable via contracts for protecting the personal confidential data they process and for meeting the National Data Guardian's data security standards.

Resources

NHS Digital resources

NHS Digital have provided a range of resources to support the introduction of the toolkit and the implementation of the data security standards. The following are available:

- About the DSPT
- Introducing the DSPT (PPP)
- DSPT for beginners
- Frequently asked questions
- DSP Toolkit – Start Guide (All Users)
- DSP Toolkit – Administrator's Guide

Accessing and registering

To access the DSPT, visit www.dsptoolkit.nhs.uk which is the DSPT home page. Select the yellow register button to register The Surgery; this requires a valid email address and practice code. Detailed guidance on the registration process can be found on page 3 of the DSP Toolkit Start Guide (hyperlinked above).

Carrying out an assessment

To complete an assessment, follow the guidance on page 10 of the DSP Toolkit start guide.

Assertions and evidence

Assertions and evidence items are specific to the organisation type. The full list of assertions and evidence items can be viewed here. The link offers guidance and tips for each assertion and is a useful reference to support staff when completing the assessment.

Practice lead

At the Surgery, the lead for the DSPT is the Data Business Analyst

Preparing staff

At The Surgery, all staff
will be given access to the referenced material to ensure they have an understanding of the requirements associated with the toolkit and are fully aware of the data security standards outlined in this document and how the standards apply in practical terms at The Surgery.

Summary

The preservation of data and information security is crucial to maintaining the trust of the entitled patient population at The Surgery. All staff have a duty to ensure that they handle information correctly and safely, in accordance with extant guidance and in line with the data security standards.

Author and Agreed By:	**Michael Hart**	**Michelle Slimm**
Job Title:	Business Data Analyst	Business Manager
Date of Issue:	January 2024	
Version Number:	V2	
Date of Review	January 2026	