Bartlett Group Practice

Data Security and Toolkit Guidance Policy

1.1.1 A. Confidentiality Notice

This document and the information contained therein is the property of Bartlett Group Practice.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Bartlett Group Practice.

BARTLETT GROUP PRACTICE	Classification :	Information Management & Technology
	Reference :	**IM&T16**
Data Security and Toolkit Guidance Policy	Issued By :	Carol Jevon
	Approved By :	Ian Friend
	Date :	03.03.2019
	Applied to sites :	Ash Vale & Frimley Green
	Applies to Staff Groups :	All Staff (Inc. Salaried GPs)

1.1.2 B. Document Revision and Approval History

Version	Date	Created By	Approved By	Comments
1.0	03.03.2019	Carol Jevon	Ian Friend	New Policy

Table of contents

2 Introduction

2.1 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. Bartlett Group Practice is required to provide assurance that they have good data security processes in place and patient information is managed appropriately.

2.2 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.

2.3 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This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time.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.

This document and any procedures contained within it are contractual and therefore form part of your contract of employment. Employees will be consulted on any modifications or change to the document's status.

2.4 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.

3 Scope

3.1 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.

3.2 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.

4 Definition of terms

4.1 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.[1]

5 Requirements

5.1 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.

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

5.2 NDG expectations

The NDG is Dame Fiona Caldicott and the requirements of the NDG are:[2]

- All staff are to ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only to be shared for lawful and appropriate purposes.
- All staff must 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 are to complete appropriate annual data security training and pass a mandatory test.

6 Data Security Standards

6.1 The ten standards

[1] NHS Digital DSP Toolkit
[2] NHS Digital DSPT e-learning

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 the safe, secure, appropriate and lawful sharing of data.[3]

The Data Security Standards are:[3]

1. 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.
2. 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.
3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the redesigned Information Governance Toolkit.
4. 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.
5. 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.
6. 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.
7. 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.
8. No unsupported operating systems, software or internet browsers are used within the IT estate.
9. 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.
10. 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.

7 Resources

7.1 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

[3] DoH Your Data: Better Security, Better Choice, Better Care

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

7.2 Accessing and registering

To access the DSPT, visit www.dsptoolkit.nhs.uk which is the DSPT homepage. Select the yellow register button to register Bartlett Group Practice; 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).

7.3 Carrying out an assessment

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

7.4 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.

7.5 Practice lead

At Bartlett Group Practice, the lead for the DSPT is Ian Friend

7.6 Preparing staff

At Bartlett Group Practice, 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 Bartlett Group Practice.

7.7 Spot check and audit

It is recommended that Bartlett Group Practice conducts regular spot checks in relation to data security, a template for which can be found at Annex A. Following the spot checks an audit should be written, the template for which can be found at Annex B.

8 Summary

The preservation of data and information security is crucial to maintaining the trust of the entitled patient population at Bartlett Group Practice. 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.

Annex A – Audit template for DSPT spot checks

Criterion	Assurance required	Source of assurance or evidence	Compliant	
			Yes	No
There is a Caldicott Guardian at the practice.	• A Caldicott Guardian has been appointed • A plan to identify confidentiality and data protection work has been developed	• Job description includes Caldicott responsibilities • Documentary evidence to support data protection work		
There is documented guidance available for staff on how to maintain confidentiality, how to keep personal information secure and the need for compliance.	• Staff understand they have a legal duty to maintain confidentiality • A confidentiality policy is in place • Staff understand the NHS Code of Practice • Staff are aware of the Caldicott Principles and how they apply in practice • Procedures are provided or referenced for the authorised disclosure of information	• Question staff to determine their level of understanding • Staff are able to access the confidentiality policy • Question staff in relation to the NHS Code of Practice • Question staff in relation to the Caldicott Principles • Ask staff to explain access request procedures		
Safe system access	• Staff understand the need to lock or log out of IT systems if leaving their desk / office • Display screens are not visible to patients or visitors	• Systems are secure if left unattended • DSE is protected and out of view of visitors or patients • No evidence of password sharing, or passwords found under workstations or keyboards		

	• Password security is maintained at all times • Smartcards are used securely	• Staff do not leave smartcards in the computer when not at their desks		
Office security	• A secure working environment is maintained at all times	• All staff are wearing visible ID badges • Access to restricted areas is controlled by key code / swipe card • Any persons not wearing ID badges are challenged by staff • Offices are secured when empty (locked) • A clear-desk routine is in place and understood by staff • Doors / windows etc. are locked		
Manual record security	• All manual records are stored appropriately	• Access to the medical records area is controlled • Record storage areas are locked when not in use / at the end of the working day		
Electronic record security	• Control measures for the security of electronic records are effective	• Only authorised persons have access to electronic records • There is no evidence of login and/or password sharing • Only current staff have access to the clinical system		

Monitoring of alerts – this includes alerts triggered through self-claimed legitimate relationships, emergency access of summary care records, etc.	• A nominated individual is in place to receive system alerts	• Alerts in regard to access to patient records are responded to appropriately		
System audits	• System audit trails are conducted on a regular basis	• A nominated member of staff conducts a system audit trail which monitors access times for users • Audits include System Audit Trail, Patient Audit Trail, and Full Audit Trail		
Restricted patient access	• Where applicable, access to patient records is restricted to only authorised staff members	• Records of access to such records are monitored to ensure that only authorised access has taken place		
Data breaches	• Failed attempts to access confidential information are recorded / reported • Data breaches are reported in line with extant guidance	• Any failed attempts to access confidential data are reported in line with practice / national policy • Staff understand how to report potential data breaches • The practice retains a record of all data breaches		
Disciplinary action	• Actions are taken in the event of 'deliberate' confidentiality or data breaches which are a result of non-compliance with policy and protocol	• A record of all actions taken, which are a result of non-compliance, is retained for audit purposes		

[Add as required]	•	•		

ACTION PLAN

	CRITERIA	ISSUE	ACTION REQUIRED TO CORRECT	BY WHOM	BY WHEN
1					
2					
3					
4					
5					

Annex B – Example of an audit report template

Bartlett Group Practice	Date of audit:	Audit reference no: [01/17] Page [1] of [2]
Summary of audit:		
Name of auditor(s):		
Date audit carried out:		
Date audit closed:		

Bartlett Group Practice	Date of audit:	Audit reference no: [01/17] Page [2] of [2]
Summary of observations:		
Observation reference:	Description of observation:	

Summary of agreed actions:		
Reference:	Action required:	By whom and date:

Agreed follow-up / review:	
Name and signature of auditor/s:	Date closed:
Additional comments:	
Name and signature of auditor/s:	Final closure date: