NHS
Somerset
NHS Foundation Trust

TOPIC ASSURANCE REPORT

REPORT DETAILS	
Topic	**Data Security and Protection (Information Governance)**
Topic Lead	Louise Coppin
Exec Lead	David Shannon
Governance Link support	Lincoln Andrews
QAG meeting date	October 2024
Period covered	1 April 2023 – 31 March 2024
Previous level(s)	**Green**
Specialist / oversight group	Data Security and Protection Group

ASSESSMENT
Recommended level **(Separate levels - an interim measure)**
Musgrove, Community, MH&LD services **Yeovil District Hospital**
Blue
Recommendation(s) for QAG follow-up

TOPIC SCOPE AND OVERSIGHT	
Scope of the topic	All organisations that have access to NHS patient data and systems must provide assurance that they are practicing good data security and that personal information is handled correctly and adhering to the National Data Guardians 10 data security standards: **Data Security Standard 1:** 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 **Data Security Standard 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. **Data Security Standard 3:** All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit. Leadership Obligation 2: Process: ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses. **Data Security Standard 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 access to personal confidential data on IT systems can be attributed to individuals. **Data Security Standard 5**: Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security. **Data Security Standard 6**: Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection. **Data Security Standard 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. Leadership Obligation 3: Technology: ensure technology is secure and up-to-date. **Data Security Standard 8**: No unsupported operating systems, software or internet browsers are used within the IT estate. **Data Security Standard 9**: A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually. **Data Security Standard 10**: IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.
Reporting Structure/ Specialist Group oversight	Data Security and Protection Group (DSPG). Quarterly meetings Chaired by David Shannon, Senior Information Risk Owner

COMPLIANCE REQUIREMENTS	
Regulation **CQC Fundamental Standards**	Completion of the Data Security and Protection Toolkit
Legislation	Data Protection Act 2018 UK General Data Protection Regulation Freedom of Information Act 2000 Records Management Code of Practice Caldicott Guidelines
National Guidance **Assessment or**	National Data Guardian data security standards Data Security and Protection Toolkit Cyber Essentials Certification

accreditation	

INTERNAL ASSURANCE – Summary information generated within the organisation

Assessing guidance and measuring the topic internally	
Self-Assessment of national guidance implementation	The Data Security and Protection Toolkit is an online self-assessment tool that allows organisation to measure their performance against the National Data Guardians 10 Data Security Standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practicing good data security, and that personal information is handled correctly. The DSPT progress is reported quarterly to the Data Security and Protection Group (DSPG). The DSPT baseline was submitted in February 2024. The Final Submission was signed off by David Shannon as SIRO and published in June 2024 with a level of 'Exceeds Standards'.
Audit and Measurement – key findings	Annual IG Audits Cyber Essentials Certification BDO Audit (February 2024)

Policy and assurance of meeting policy standards	
Policy and review status	Data Protection and Information Governance Policy Freedom of Information Policy Data Protection Impact Assessment Policy Information Security Suite of Policies
Monitoring policy compliance	Annual IG audits care carried out to monitor compliance and knowledge.

Colleagues: Training and competencies	
Training and competency requirements	All staff who handle personal data are required to complete annual data security training. The data security training is provided by NHSE via the LEAP platform.
Training Compliance	The training compliance rate required by the DSPT is 90% Our current training compliance is at 94%.

EXTERNAL ASSURANCE – Summary of topic-relevant feedback	
External Reviews / Assessments	Cyber Essentials Certification BDO Audit (February 2024)
External / Internal organisational Audits	Our DSPT was audited by BDO in February 2024 using the criteria provided by NHSE for auditing the DSPT including a set list of assertions. The Audit found that the evidence provided for 42 of the 45 mandatory sub-assertions was found to be satisfactory and in line with the requirements of the independent assessment framework. There was insufficient evidence to completely support, at the time of the audit, 3 of the 45 mandatory sub-assertions included in the sample. Which were rectified prior to the final submission in June. BDO rated confidence in the Trust's DSP Toolkit return as high because they noted that the work completed on the DSP Toolkit has been in line with the requirements of the DSP Toolkit, with some minor deviations, and the Trust's latest self-assessment was 'Standards Exceeded'. The Final Submission was signed off by David Shannon as SIRO and published in June 2024 with a level of 'Exceeds Standards'.
National Audits / Surveys	N/A

ENGAGEMENT AND INVOLVEMENT	
Colleague engagement	Annual IG audits are carried out by all departments to identify good practice, compliance with policies, knowledge and risks/issues.
Patient and public involvement	N/A

ONGOING ISSUES & ACTIONS	
Current Issues	Due to a significant increase in the number of requests and staffing issues, there is a backlog of data access requests causing problems with compliance requirement of one calendar month. We are monitoring staffing levels, increasing our workforce, reviewing processes and identifying if different systems would help these issues. The Information Commissioner's Office (ICO) is aware of our backlog and our continued efforts to rectify this issue. Currently we have approximately 860 requests with 600 overdue. 2023/24 compliance was 50%.
Integration status	The information governance team is now fully integrated including: • Training packages and training requirements

	• Annual IG Audits • Documentation • Data Security and Protection Toolkit • Data security and Protection Group • Freedom of Information processes • Subject Access Request processes • Information Asset Register • Data flows
Topic-related Risks	Due to increased numbers of requests and staffing issues, there is a backlog of subject access requests causing problems with compliance requirement of one calendar month. We are monitoring staffing levels and reviewing processes and identifying if different systems would help these issues.
Action plan delivery	

Other Supporting Information

We have maintained the standard of ‘Exceeds Standards’ within the Data Security Protection Toolkit for a number of years. The format of the Toolkit is due to change for the next submission in June 2025 and will be more focused on the Cyber Assessment Framework.

We have developed and implemented a new Information Asset Register. This was implemented in May 2024 and is currently 98% complete. All 490 active Assets have an Information Asset Owner and an Information Asset Administrator. Each Asset is registered with details of security, clinical safety, contract and procurement information.