Enclosure 10

TOPIC ASSURANCE REPORT

REPORT DETAILS	
Topic	**Data Security and Protection (Information Governance)**
Topic Lead	Louise Coppin
Exec Lead	Phil Brice
Governance Link support	Lincoln Andrews
QAG meeting date	09 August 2023
Period covered	July 2022 to June 23
Previous level(s)	
Specialist / oversight group	Data Security and Protection Group

ASSESSMENT	
Recommended level (Separate levels - an interim measure)	
Musgrove, Community, MH&LD services	**Yeovil District Hospital**
G	A
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

Use this section to indicate the key requirements we must seek to meet for the topic
This does not need to be a comprehensive listing – what are most critical requirements?

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	National Data Guardian data security standards

Assessment or accreditation	Data Security and Protection Toolkit Cyber Essentials Certification

Use this section to summarise the assurance available from all internal sources of evidence / information

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 2023. The Final Submission was signed off by David Shannon as SIRO and published in June 2023 with a level of ‘Exceeds Standards’. The Final submission was for SFT as a whole (we were not required to submit a toolkit for YDH as they ceased to exist as a legal entity by this time.
Audit and Measurement – key findings	Annual IG Audits Cyber Essentials Certification BDO Audit

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 95% Our current training compliance is at 93%.

Use this section to summarise the assurance available from feedback that external agencies, auditors and benchmarked data sources

EXTERNAL ASSURANCE – Summary of topic-relevant feedback	
External Reviews / Assessments	Cyber Essentials Certification BDO Audit
External / Internal organisational Audits	Our DSPT was audited by BDO in February 2023 using the criteria provided by NHSE for auditing the DSPT including a set list of assertions. The Audit found that the evidence provided for 47 of the 49 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, 2 of the 49 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'. Detailed findings and recommendations (page 5) and the management responses can be found within the attached report. The Final Submission was signed off by David Shannon as SIRO and published in June 2023 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

Use this section to summarise issues and risks impacting on the topic and any improvement plans in place

Enclosure 10

ONGOING ISSUES & ACTIONS	
Current Issues	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. The Information Asset Register is not currently up to date – an in-house database is being built with an expected implementation date of January to ensure compliance.
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 Outstanding Policies are the Data Protection and Information Governance policy which is currently being reviewed.
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. The Information Asset Register is not currently up to date – an in-house database is being built with an expected implementation date of January to ensure compliance.
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. Freedom of Information compliance is currently at approximately 80% per month (this was an average of 60% for SFT and 55% for YDH through 22/23).

Enclosure 10

Reference – Assurance level definitions

Green	Blue	Amber	Red
Definition – assurance / concern characteristics			
Good systems of assurance High confidence in the quality of the evidence available. Positive findings from measurement / assessment / monitoring sources, minimal variability. No significant concerns in the period covered.	Assurance systems in place – adequately functioning. Sufficient confidence in the quality of the evidence available. Acceptable findings from measurement / assessment / monitoring sources, acceptable variability. No evidence of any significant issues in the period. Any issues /concerns are well-managed via clear, monitored plans.	Assurance systems in place – issues evident with functioning. Lower confidence in the quality of evidence / due to gaps in information available Findings from measurement / assessment / monitoring sources indicate concerns / variability. Issues of concern are not accompanied by assurance of clear, monitored plans to address.	Assurance systems are not adequately designed and/or not all functioning well. Concerning low quality of evidence, significant gaps. Findings from measurement / assessment / monitoring sources indicate concerns warranting escalation. Serious issues identified that present risks to the Trust and in the absence of an effective plan to address.
Application of the level – guidance and conventions **The level applies when..**			
There is agreement that there is overall high confidence that all is well. Minor issues only. An external review today would likely find no issues.	There is agreement that sufficient confidence that all is well. Issues can be left with the Lead to take forward. An external review today likely to find issues are managed.	The consensus is that improvements are required before there can be fuller confidence. Issues may require support to resolve. An external review today may find concerns and weaknesses in managing them.	It is evident that all is not well. Issues warrant escalation to achieve resolution. An external review today would find concerns and would likely take action.
Onward reporting conventions			
At one year - Light-touch update report	At one year – Update briefing with focus on actions progress – targeting the issues previously reported and any new issues arising since	On consensus from QAG review: At six months - An update on areas of concern and position update on improvement planning At one year – An update as above accompanied by an updated assurance report	On consensus from QAG review: Within 1 month - Specific briefing provided to accountable Executive and other relevant leads or stakeholders. Topic review meeting held 1-6 months. Aim – to support development and improvement to address issues / concerns At one year – Full updated assurance report reflecting progress and plans
Templates			
Simple update briefing	Issue-specific briefing / progress briefing	Issue-specific briefing / progress briefing Assurance report (update)	Escalation briefing / progress briefing and SMART plan Assurance report