Maidstone and
Tunbridge Wells
NHS Trust

Ref: FOI/GS/ID 6852

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone, Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net
www.mtw.nhs.uk

20 July 2021

Freedom of Information Act 2000

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to Data Security and Protections Toolkit.

You asked:
For the Data Security and Protection Toolkit you were required to have an independent audit on your toolkit return.
Please confirm:-

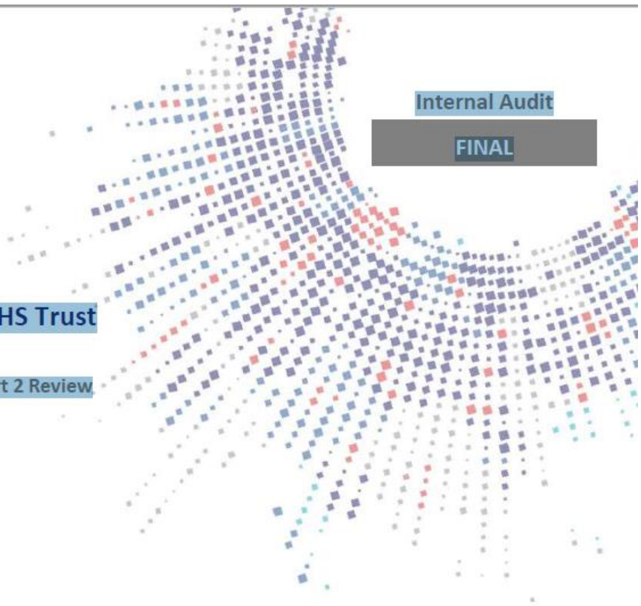
1. *Did you have an audit on your DSP Toolkit in line with the Strengthening Assurance Framework from NHS Digital?*
2. *How much did this cost?*
3. *What was the audit?*
4. *What was the score?*

Trust response:
1. Yes
2. This forms part of our annual audit fee with TIAA. Under Section 21 of the Act we are not required to provide information in response to a request if the information is already reasonably accessible to you. The information you requested is available from the trust website using the following link/s: http://www.mtw.nhs.uk/wp-content/uploads/2021/06/Trust-Board-agenda-and-reports-June-2021-at-22.06.21.pdf p536
3. Please see attached report
4. Please see attached report

tiaa

Internal Audit

FINAL



Maidstone and Tunbridge Wells NHS Trust

Data Security and Protection Toolkit (DSPT) Part 2 Review

2020/21

June 2021

tiaa

Executive Summary

OVERALL ASSESSMENT

Overall Risk Rating across the 10 Data Standards:

Confidence Level	Overall Risk Rating
High	Substantial

Number of Data Standards which are -

Substantial	Moderate	Limited	Unsatisfactory
10	0	0	0

Number of findings which are –

Low	Medium	High	Critical
2	0	0	0

KEY STRATEGIC FINDINGS

- Policies reviewed were found to be up to date.
- 105 out of 110 evidence items have been completed to date.
- Outstanding items are due to be completed by the submission date, and are currently in progress.

GOOD PRACTICE IDENTIFIED

- There is a Governance Framework in place. Information Governance is overseen by the Information Governance Committee.

ASSURANCE OVER KEY STRATEGIC RISK / OBJECTIVE

The review followed the draft Data Security and Protection (DSP) Toolkit Independent Assessment Framework and Guidance published by NHS Digital. TIAA have reviewed 13 assertions across the 10 National Data Guardian Standards in the DSP Toolkit. These assertions were pre-determined as in-scope by NHS Digital.

SCOPE

TIAA undertook an independent audit of the organisation's 10 Data Security Standards. The audit coverage was aligned to the mandated areas in the toolkit as selected by NHS Digital for 2020-2021. The DSP Toolkit submissions are also included as part of the CQC's Well-Led inspections. These standards address modern data security threats as well as inherent information governance processes operated at NHS organisations.

Findings and Recommendations

Overall Rating for Finding 1		Low
Related assertions:		Standard 1 (Assertion 6)
Finding text and explanation	To provide the overall findings of the last data protection by design audit.	
Finding	Not yet completed on the Toolkit. A third party was commissioned to do this and report is awaited, held up by staff sickness. Anticipate receipt of the report will be mid-June.	
Implications	The evidence item is not completed.	
Recommendations	Awaiting receipt of report, then Toolkit can be updated.	

Overall Rating for Finding 2		Low
Related assertions:		Standard 9 (Assertion 2)
Finding text and explanation	To confirm the date the penetration test and vulnerability scan was undertaken.	
Finding	The Pen Test is to be carried out in two parts - remotely during May, and onsite during June. The report will be available week commencing 14 June for sign off by SIRO by submission date.	
Implications	The evidence item is not completed.	
Recommendations	To complete evidence item on the Toolkit once sign off undertaken.	

Data Standards, Assertions and Evidence Items

This section has been split into three sections –

- Data Standards;
- Assertions;
- Evidence Items.

There are 10 Data Standards per Toolkit. Each Data Standard is split into Assertions, and each Assertion is split into Evidence Items (110 mandatory).

Section 1 - Data Standards

Summary of Data Standards Risk Ratings

Standard	Risk Rating	Overall Risk Rating
1	Substantial	Substantial
2	Substantial	
3	Substantial	
4	Substantial	
5	Substantial	
6	Substantial	
7	Substantial	
8	Substantial	
9	Substantial	
10	Substantial	

Section 2 - Assertions

Thirteen mandatory assertions were reviewed in line with NHS Digital's 2020/21 Audit Scope. The coverage included 1.6, 1.8, 2.2, 3.1, 4.2, 5.1, 6.2, 7.2, 7.3, 8.3, 8.4, 9.2 & 10.2.

Summary of Assertion Risk Ratings

DSS 1 –Personal Confidential Data

Assertion	NDG Rating:	NDG Score:
1.6	Low	1
1.8	Not Reportable	0
Mean score:		0.5
DSS Risk Rating:		Substantial

DSS2 – Staff Responsibilities

Assertion	NDG Rating:	NDG Score:
2.2	Not Reportable	0
Mean score:		0
DSS Risk Rating:		Substantial

DSS 3 - Training

Assertion	NDG Rating:	NDG Score:
3.1	Not Reportable	0
Mean score:		0
DSS Risk Rating:		Substantial

DSS 4 – Managing Data Access

Assertion	NDG Rating:	NDG Score:
4.2	Not Reportable	0
Mean score:		0
DSS Risk Rating:		Substantial

DSS 5 – Process Reviews

Assertion	NDG Rating:	NDG Score:
5.1	Not Reportable	0
Mean score:		0
DSS Risk Rating:		Substantial

DSS 6 – Responding to Incidents

Assertion	NDG Rating:	NDG Score:
6.2	Not Reportable	0
Mean score:		0
DSS Risk Rating:		Substantial

DSS 7 – Continuity Planning

Assertion	NDG Rating:	NDG Score:
7.2	Not Reportable	0
7.3	Not Reportable	0
Mean score:		0
DSS Risk Rating:		Substantial

DSS 8 – Unsupported Systems

Assertion	NDG Rating:	NDG Score:
8.3	Not Reportable	0
8.4	Not Reportable	0
Mean score:		0
DSS Risk Rating:		Substantial

DSS 9 – IT Protection

Assertion	NDG Rating:	NDG Score:
9.2	Low	1
Mean score:		1
DSS Risk Rating:		Substantial

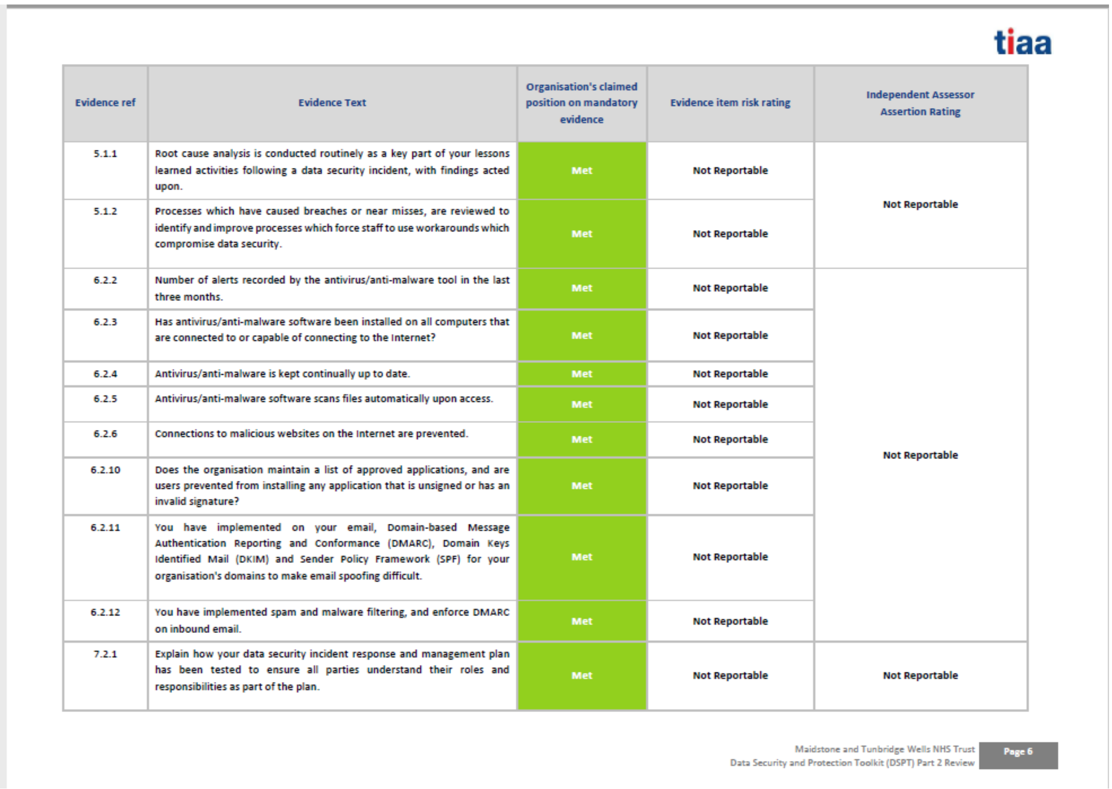
DSS 10 – Accountable Suppliers

Assertion	NDG Rating:	NDG Score:
10.2	Not Reportable	0
Mean score:		0
DSS Risk Rating:		Substantial

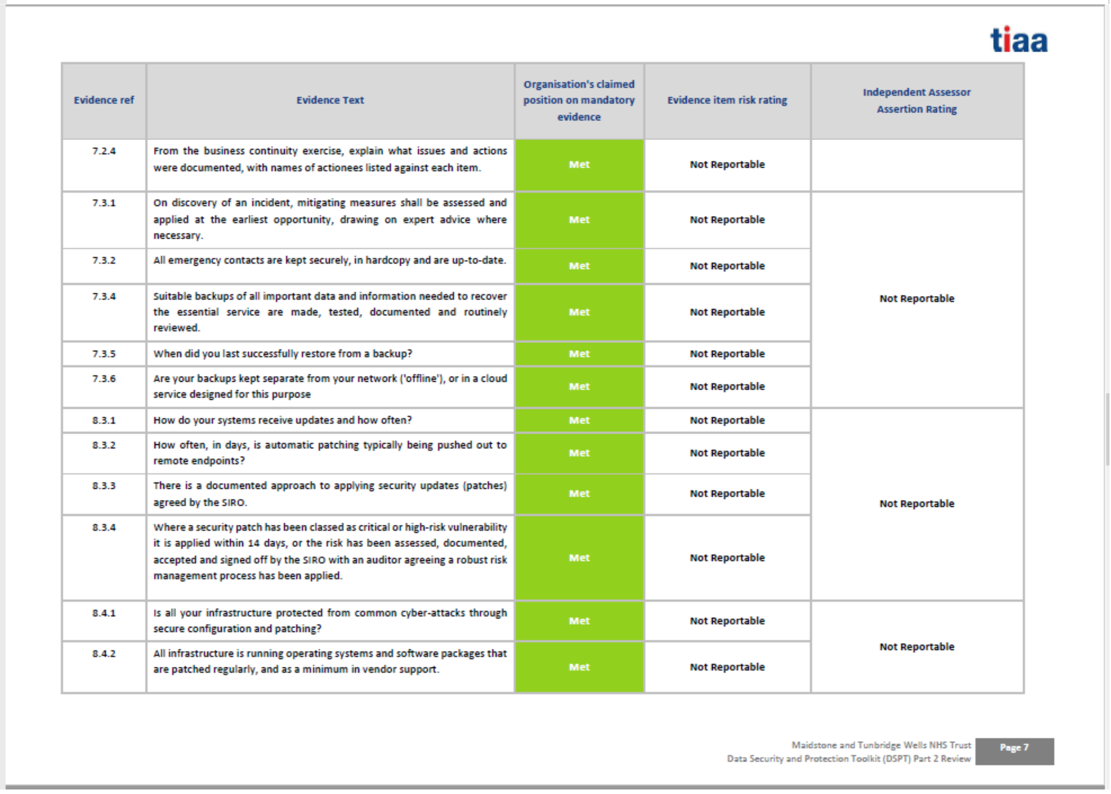
Section 3 - Evidence Items

Summary of Evidence Items Claimed Positions and Auditor Conclusion

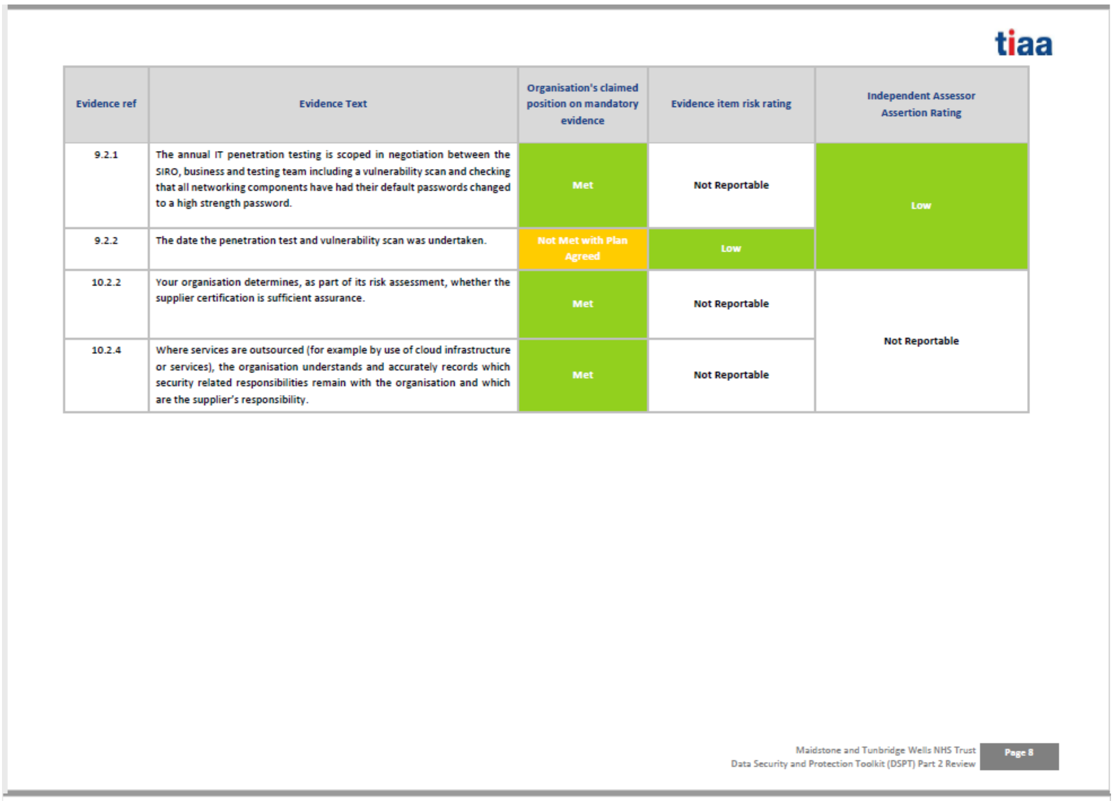
Evidence ref	Evidence Text	Organisation's claimed position on mandatory evidence	Evidence item risk rating	Independent Assessor Assertion Rating
1.6.1	Is there is an approved procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements?	Met	Not Reportable	Low
1.6.2	There are technical controls that prevent information from being inappropriately copied or downloaded.	Met	Not Reportable	
1.6.3	There are physical controls that prevent unauthorised access to buildings and locations where personal data are stored or processed.	Met	Not Reportable	
1.6.4	Provide the overall findings of the last data protection by design audit.	Not Met with Plan Agreed	Low	
1.8.1	Does your organisation operate and maintain a data security risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility?	Met	Not Reportable	Not Reportable
1.8.3	What are your top three data security and protection risks?	Met	Not Reportable	
2.2.1	Is there a data protection and security induction in place for all new entrants to the organisation?	Met	Not Reportable	Not Reportable
2.2.2	Do all employment contracts contain data security requirements?	Met	Not Reportable	
3.1.1	Has an approved organisation-wide data security and protection training needs analysis been completed after 1 April 2020?	Met	Not Reportable	Not Reportable
4.2.1	When was the last audit of user accounts held?	Met	Not Reportable	Not Reportable
4.2.3	Logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity.	Met	Not Reportable	
4.2.5	Are unnecessary user accounts removed or disabled?	Met	Not Reportable	



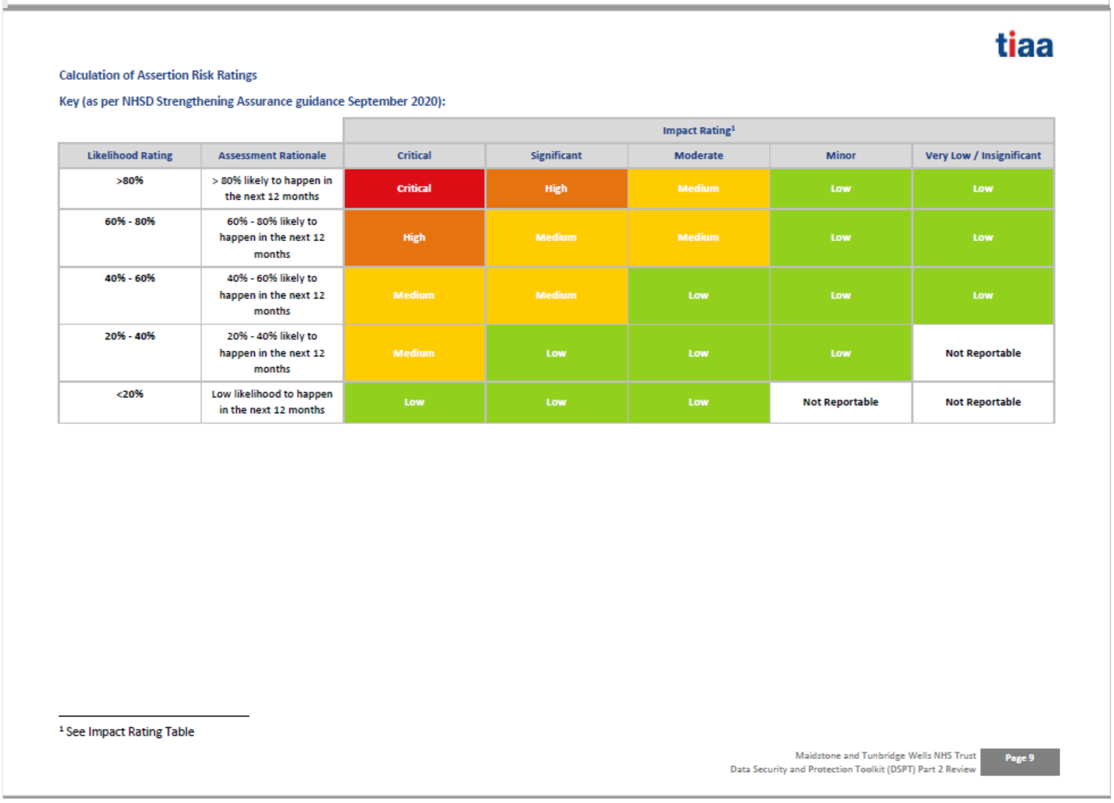
Evidence ref	Evidence Text	Organisation's claimed position on mandatory evidence	Evidence item risk rating	Independent Assessor Assertion Rating
5.1.1	Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security incident, with findings acted upon.	Met	Not Reportable	Not Reportable
5.1.2	Processes which have caused breaches or near misses, are reviewed to identify and improve processes which force staff to use workarounds which compromise data security.	Met	Not Reportable	
6.2.2	Number of alerts recorded by the antivirus/anti-malware tool in the last three months.	Met	Not Reportable	Not Reportable
6.2.3	Has antivirus/anti-malware software been installed on all computers that are connected to or capable of connecting to the Internet?	Met	Not Reportable	
6.2.4	Antivirus/anti-malware is kept continually up to date.	Met	Not Reportable	
6.2.5	Antivirus/anti-malware software scans files automatically upon access.	Met	Not Reportable	
6.2.6	Connections to malicious websites on the Internet are prevented.	Met	Not Reportable	
6.2.10	Does the organisation maintain a list of approved applications, and are users prevented from installing any application that is unsigned or has an invalid signature?	Met	Not Reportable	
6.2.11	You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your organisation's domains to make email spoofing difficult.	Met	Not Reportable	
6.2.12	You have implemented spam and malware filtering, and enforce DMARC on inbound email.	Met	Not Reportable	
7.2.1	Explain how your data security incident response and management plan has been tested to ensure all parties understand their roles and responsibilities as part of the plan.	Met	Not Reportable	Not Reportable



Evidence ref	Evidence Text	Organisation's claimed position on mandatory evidence	Evidence item risk rating	Independent Assessor Assertion Rating
7.2.4	From the business continuity exercise, explain what issues and actions were documented, with names of actionees listed against each item.	Met	Not Reportable	
7.3.1	On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary.	Met	Not Reportable	Not Reportable
7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Met	Not Reportable	
7.3.4	Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.	Met	Not Reportable	
7.3.5	When did you last successfully restore from a backup?	Met	Not Reportable	
7.3.6	Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose	Met	Not Reportable	
8.3.1	How do your systems receive updates and how often?	Met	Not Reportable	Not Reportable
8.3.2	How often, in days, is automatic patching typically being pushed out to remote endpoints?	Met	Not Reportable	
8.3.3	There is a documented approach to applying security updates (patches) agreed by the SIRO.	Met	Not Reportable	
8.3.4	Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.	Met	Not Reportable	
8.4.1	Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?	Met	Not Reportable	Not Reportable
8.4.2	All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.	Met	Not Reportable	



Evidence ref	Evidence Text	Organisation's claimed position on mandatory evidence	Evidence item risk rating	Independent Assessor Assertion Rating
9.2.1	The annual IT penetration testing is scoped in negotiation between the SIRO, business and testing team including a vulnerability scan and checking that all networking components have had their default passwords changed to a high strength password.	Met	Not Reportable	Low
9.2.2	The date the penetration test and vulnerability scan was undertaken.	Not Met with Plan Agreed	Low	
10.2.2	Your organisation determines, as part of its risk assessment, whether the supplier certification is sufficient assurance.	Met	Not Reportable	Not Reportable
10.2.4	Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility.	Met	Not Reportable	



Calculation of Assertion Risk Ratings

Key (as per NHSD Strengthening Assurance guidance September 2020):

		Impact Rating[1]				
Likelihood Rating	Assessment Rationale	Critical	Significant	Moderate	Minor	Very Low / Insignificant
>80%	> 80% likely to happen in the next 12 months	Critical	High	Medium	Low	Low
60% - 80%	60% - 80% likely to happen in the next 12 months	High	Medium	Medium	Low	Low
40% - 60%	40% - 60% likely to happen in the next 12 months	Medium	Medium	Low	Low	Low
20% - 40%	20% - 40% likely to happen in the next 12 months	Medium	Low	Low	Low	Not Reportable
<20%	Low likelihood to happen in the next 12 months	Low	Low	Low	Not Reportable	Not Reportable

[1] See Impact Rating Table

Impact Rating Table

Impact rating	Assessment rationale
Critical	A **Critical Impact Finding** could apply to Health and Social Care organisations that use extremely complex technologies to deliver multiple services or process large volumes of patient data, including processing for other organisations. Many of the services are at the highest level of risk, including those offered to other organisations. New and emerging technologies are utilised across multiple delivery channels. The organisation is responsible for/ maintains nearly all connection types to transfer/store/process personal, patient identifiable and/or business-critical data with customers and third parties. A Critical finding that could have a: • Critical impact on operational performance or the ability to deliver services / care; or • Critical monetary or financial statement impact;or • Critical breach in laws and regulations that could result in material fines or consequences; or • Critical impact on the reputation or brand of the organisation which could threaten its future viability.
Significant	A **Significant Impact Finding** could apply to a Health and Social Care organisation that use complex technology in terms of scope and sophistication. The organisation may offer high-risk products and services that may include emerging technologies. The organisation is responsible for/ maintains the largest proportion of connection types to transfer/store/process personal, patient identifiable or business-critical data with customers and third parties; other organisations and/or third-parties are responsible for/maintain a low proportion of connection types. A Significant finding that could have a: • Significant impact on operational performance;or • Significant monetary or financial statement impact;or • Significant breach in laws and regulations resulting in large fines and consequences; or • Significant impact on the reputation or brand of theorganisation.
Moderate	A **Moderate Impact Finding** could apply to a Health and Social Care organisation that uses technology which may be somewhat complex in terms of volume and sophistication. The organisation is responsible for/maintains some connection types to transfer/store/process personal, patient identifiable and/or business- critical data with customers and third parties; other organisations and/or third-parties are responsible for/maintain a most of the organisation's connection types. A Moderate finding that could have a: • Moderate impact on the organisation's operational performance;or • Moderate monetary or financial statement impact;or • Moderate breach in laws and regulations with moderate consequences;or • Moderate impact on the reputation of the organisation.
Minor	A **Minor Impact Finding** could apply to a Health and Social Care organisation with limited complexity in terms of the technology it uses. It offers a limited variety of less risky products and services. The institution primarily uses established technologies. It is responsible for/maintains minimal numbers of connection types to transfer/store/process personal, patient identifiable or business-critical data too customers and third parties; other organisations and/or third-parties are largely responsible for/maintain connection types. A Minor finding that could have a: • Minor impact on the organisation's operational performance; or • Minor monetary or financial statement impact; or • Minor breach in laws and regulations with limited consequences; or • Minor impact on the reputation of the organisation.
Very Low Insignificant	A **Low Impact Finding** could apply to a Health and Social Care organisation that has very limited use of technology. The variety of products and services are limited and the organisation has a small geographic footprint with few employees. It is responsible for/maintains no connection types to transfer/store/process personal, patient identifiable or business-critical data too customers and third parties. A Low finding that could have a: • Insignificant impact on the organisation's operational performance; or • Insignificant monetary or financial statement impact; or • Insignificant breach in laws and regulations with little consequence; or Insignificant impact on the reputation of the organisation.

EXPLANATORY INFORMATION

Appendix A

Scope and Limitations of the Review

1. The definition of the type of review, the limitations and the responsibilities of management in regard to this review are set out in the Annual Plan. As set out in the Audit Charter, substantive testing is only carried out where this has been agreed with management and unless explicitly shown in the scope no such work has been performed.

Disclaimer

2. The matters raised in this report are only those that came to the attention of the auditor during the course of the review, and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

Acknowledgement

3. We would like to thank staff for their co-operation and assistance during the course of our work.

Release of Report

4. The table below sets out the history of this report.

Stage	Issued	Response Received
Audit Planning Memorandum:	25th November 2020	25th November 2020
Draft Report:	4th June 2021	8th June 2021
Final Report:	10th June 2021	

Confidence Level

Key (as per NHSD Strengthening Assurance guidance September 2020):

Level of deviation from the DSP Toolkit submission and assessment findings	Confidence level
High level of deviation - the organisation's self-assessment against the Toolkit differs significantly from the Independent Assessment For example, the organisation has declared as "Standards Met" or "Standards Exceeded" but the independent assessment has found individual NDG standards as 'Unsatisfactory' and the overall rating is 'Unsatisfactory'.	Low
Medium level of deviation - the organisation's self-assessment against the Toolkit differs somewhat from the Independent Assessment For example, the Independent Assessor has exercised professional judgement in comparing the self-assessment to their independent assessment and there is a non-trivial deviation or discord between the two.	Medium
Low level of deviation- the organisation's self-assessment against the Toolkit does not differ / deviates only minimally from the Independent Assessment	High

Overall Risk Rating

Key (as per NHSD Strengthening Assurance guidance September 2020):

Overall risk rating across all in-scope standards	
Unsatisfactory	1 or more Standards is rated as 'Unsatisfactory'
Limited	No standards are rated as 'Unsatisfactory', but 2 or more are rated as 'Limited'
Moderate	There are no standards rated as 'Unsatisfactory', and 1 or none rated as 'Limited'. However, not all standards are rated as 'Substantial'.
Substantial	All of the standards are rated as 'Substantial'

AUDIT PLANNING MEMORANDUM

Appendix B

Client:	Maidstone and Tunbridge Wells NHS Trust
Review:	Data Security and Protection Toolkit v3
Type of Review:	ICT Audit
Review Agreed By:	In the Annual Plan 2020/21

Planned Start Date:	Part 1 – 8th March 2021 Part 2 – 3rd May 2021
Planned Exit Meeting Date:	Part 1 – March 2021 Part 2 – May 2021

Lead Auditor:	Paul Merison, Director of ICT Audit
Exit Meeting to be held with:	Gail Spinks, Head of Information Governance gspinks@nhs.net

SELF ASSESSMENT RESPONSE

Matters over the previous 12 months relating to activity to be reviewed (to be covered at the opening meeting).	Y/N
Has there been any reduction in the effectiveness of the internal controls due to staff absences through sickness and/or vacancies etc?	
Have there been any breakdowns in the internal controls resulting in disciplinary action or similar?	
Have there been any significant changes to the process?	
Are there any particular matters/periods of time you would like the review to consider?	

Detailed scope will consider:	Directed	Delivered
	• Documented • Risk Mitigation • Compliance	• Performance monitoring • Reputational • Financial control

Outline scope (per Annual Plan):

NHS Digital have published their "Strengthening Assurance – Independent Assessment Guidance" for assurance reviews of NHS organisations' Data Security and Protection Toolkits. The release accompanying this guidance confirms that these annual audits are a mandatory requirement.

Detailed scope / requested additions to the scope

TIAA will undertake an independent audit of the Trust's 10 Data Security Standards. The audit coverage will be aligned to the mandated areas in the toolkit as selected by NHS Digital for 2020-2021. Our review is a two part assessment with a Part 1 Status Update report which does not include the audit opinion and a second visit resulting in a full report showing DSS risk scores and the audit opinion. The DSP Toolkit submissions are also included as part of the CQC's Well-Led inspections.

These standards address modern data security threats as well as inherent information governance processes operated at NHS organisations.

Detailed scope / requested additions to the scope - continued

The review will test the mandatory evidence items relating to the following assertions as directed by NHS Digital:

DSS	Summary Description	2020-21 audit coverage (assertions)
1	Staff ensure that personal confidential data is handled, stored and transmitted securely.	1.6, 1.8
2	All staff understand their responsibilities for Data Security.	2.2
3	All staff complete annual data security training and pass a mandatory test.	3.1
4	Personal confidential data is only accessible to staff who need it.	4.2
5	Processes that have caused breaches or near misses are reviewed annually.	5.1
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.	6.2
7	A continuity plan is in place, tested annually, with a report to senior management.	7.2, 7.3
8	No unsupported operating systems, software or internet browsers are used.	8.3, 8.4
9	A strategy for protecting IT systems from cyber threats is in place and reviewed annually.	9.2
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.	10.2

Information / documentation request

Online access to the DSPT will be required for the Auditor and Director of ICT Audit.