Data Security and Protection Toolkit Assessment Summary Report 2020/21 (Final)

Walton Centre NHS Foundation Trust

Report Ref: 108WCFT_2021_902

Date of Issue: June 2021

Contents

Limitations

The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required. Whilst every care has been taken to ensure that the information in this report is as accurate as possible, based on the information provided and documentation reviewed, no complete guarantee or warranty can be given with regards to the advice and information contained herein. Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

Responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

Reports prepared by MIAA are prepared for your sole use and no responsibility is taken by MIAA or the auditors to any director or officer in their individual capacity. No responsibility to any third party is accepted as the report has not been prepared for, and is not intended for, any other purpose and a person who is not a party to the agreement for the provision of Internal Audit and shall not have any rights under the Contracts (Rights of Third Parties) Act 1999.

Future periods

The assessment of controls relating to the process is that at June 2021. Historic evaluation of effectiveness is not always relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in the operating environment, law, regulation or other; or
- The degree of compliance with policies and procedures may deteriorate.

Public Sector Internal Audit Standards

Our work was completed in accordance with Public Sector Internal Audit Standards.

Key Dates

Report Stage	Date
Discussion Document Issued	28/06/2021
Final Draft Report Issued	01/07/2021
Client Approval Received	08/07/2021
Final Report Issued	07/07/2021

Report Distribution

Name	Title
Mike Burns	Director of Finance & IT (SIRO)
Andy Nicolson	Medical Director (Caldicott Guardian)
Justin Griffiths	Head of IM&T
Lorraine Blyth	Digital Health Records & IG Manager

Audit Team

Name	Contact Details	
Michael McCarthy	Michael.McCarthy@miaa.nhs.uk	07552 258 920
Gemma Owens	Gemma.Owens@miaa.nhs.uk	07717 720 389
Paula Fagan	Paula.Fagan@miaa.nhs.uk	07825 592 866

Acknowledgement and Further Information

MIAA would like to thank all staff for their co-operation and assistance in completing this review. This report has been prepared as commissioned by the organisation, and is for your sole use. If you have any queries regarding this review please contact the Audit Manager. To discuss any other issues then please contact the Director. MIAA would be grateful if you could complete a short survey using the link below to provide us with valuable feedback to support us in continuing to provide the best service to you.
https://www.surveymonkey.com/r/MIAA_Client_Feedback_Survey

1 Introduction, Background and Objective

In 2018 the Information Governance toolkit (IGT) was withdrawn and replaced with the new Data Security and Protection Toolkit (DSPT). It was developed by NHS Digital in response to The National Data Guardian's Review of Data Security, Consent and Opt-Outs published in July 2016 and the subsequent Government response, Your Data: Better Security, Better Choice, Better Care, published in July 2017.

The DSPT is a tool which allows organisations to measure their compliance against legislation and central guidance, and helps identify areas of full, partial or non-compliance.

In September 2020, NHS Digital published a methodology for independent assessment and internal audit providers to implement when performing DSPT audits (https://www.dsptoolkit.nhs.uk/News/83) which included a set scope for the review.

The published assessment methodology requires assessors/auditors to form a view on the in-scope assertions and key elements of your DSP Toolkit environment including:

- An assessment of the overall risk associated with the organisation's data security and data protection control environment. i.e. the level of risk associated with controls failing and data security and protection objectives not being achieved;
- An assessment as to the veracity of the organisation's self-assessment / DSP Toolkit submission and the assessor's level of confidence that the submission aligns to their assessment of the risk and controls.

The guidance also provides a reporting and scoring standard.

Whilst this guidance has formed the basis of our approach, we have had to apply flexibility and pragmatism to the approach given the impacts and challenges of delivering this review during the height of the third wave of coronavirus pandemic. As such, review and assessment in some instances has been based on evidence as provided rather than that independently obtained.

2 Scope

In accordance with the guidance mandated by NHS Digital, the selected thirteen DSPT assertions assessed during this review were:

Area	Description
1.6	The use of personal information is subject to data protection by design and by default.
1.8	There is a clear understanding and management of the identified and significant risks to sensitive information and services
2.2	Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.
3.1	There has been an assessment of data security and protection training needs across the organisation.
4.2	Organisation assures good management and maintenance of identity and access control for its networks and information systems
5.1	Process reviews are held at least once per year where data security is put at risk and following data security incidents.
6.2	All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.
7.2	There is an effective test of the continuity plan and disaster recovery plan for data security incidents.
7.3	You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.
8.3	Supported systems are kept up-to-date with the latest security patches.
8.4	You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.
9.2	A penetration test has been scoped and undertaken

Area	Description
10.2	Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS Digital guidance.

The scope of this review included only the mandatory elements of the above selected assertions.

3 Executive Summary

In the first year of the DSPT, 2018/19, the Trust met the standards. In 2019/20, the Trust again submitted a Standards Met assessment.

The Trust has demonstrated that it has plans for completion of its toolkit submission in time for the June 2021 submission including reporting of its baseline position

3.1 Areas of good practice

During our review we noted the following areas of good practice:

- The Trust had evidence of data protection by design audits being undertaken during the year under review.
- There was a Risk Management Policy in operation at the Trust which included the management of Information Governance and IT risks.
- The Trust could evidence a training needs analysis was in place during 2020-21 which included all staff and specialist IG role training requirements.
- There was evidence of ongoing monitoring of the Trust's IT estate in respect of anti-virus installation and patch management.
- Domain-based Message Authentication Reporting Conformance (DMARC) was enforced on the organisations email system.
- Testing on a sample of CareCERTs found that each had been remedied within 14 days of publication from NHS Digital.
- The Trust have recently reimplemented an offline backup solution for critical systems including EPR, PAS and pathology however it is noted that these arrangements should be formally risk assessed to ensure they provide appropriate protection to Trust data in the event of a ransomware attack.

3.2 Areas of vulnerability and/or where improvement is required

Our detailed findings and recommendations are described in more detail in a spreadsheet that has been provided under separate cover in order that vulnerabilities are not described in detail within this document. The spreadsheet should be treated as confidential as disclosure, without significant redaction, may result in any vulnerabilities becoming more widely known and exploited.

The key areas identified, however, can be summarised thus:

- During sample testing on user account access for terminations, it was identified that one account remained active and we were informed this was a decision by the IT team due to the importance of the ex-employee's role until a replacement was appointed. We were not provided any further evidence of assurance the Trust had that the ex-employee did not retain access to their account following their termination date.
- The Trust had not formally documented its controls in relation to web proxy and data loss prevention.
- The Vulnerability Management Policy could be strengthened to document the Trust's anti-virus processes in relation to managing alerts.

- It was found that there were no Recovery Time Objectives (RTOs) or Recovery Point Objectives (RPOs) agreed with system owners across the Trust.
- The Trust relies on virtual patching for out of support operating systems, such as Windows Server 2008. Whilst it is noted this does mitigate some risk, removal of end of support operating systems would be more secure.
- The Trust did not have a documented process for the monitoring of supplier certifications following onboarding.

4 Assessment and Assurance

4.1 Assessment of self-assessment

In our view, the organisation's self-assessment against the Toolkit deviates only minimally from the Independent Assessment and, as such, the assurance level in respect of the veracity of the self-assessment is:

Substantial

4.2 Assessment against National Data Guardian Standards

Across the National Data Guardian Standards our assurance ratings, based upon criteria at Appendix B are:

National Data Guardian Standard level	Overall assurance rating at the National Data Guardian level
1. Personal Confidential Data	Substantial
2. Staff Responsibilities	Substantial
3. Training	Substantial
4. Managing Data Access	Substantial
5. Process Reviews	Substantial
6. Responding to Incidents	Substantial
7. Continuity Planning	Substantial
8. Unsupported Systems	Substantial
9. IT Protection	Substantial
10. Accountable Suppliers	Substantial

The rating is based on a mean risk rating score at the National Data Guardian (NDG) standard level. Scores have been calculated using the guidance from the independent assessment Guidance document.

As a result of the above, our overall assurance level across all 10 NDG Standards is rated as:

Substantial

Appendix A: Terms of Reference

Our work aimed to assess and provide assurance based upon the validity of the organisation's intended final submission, and consider not only if the submission is reasonable based on the evidence submitted, but also provide assurance based on the extent to which information risk has been managed in this context.

Our scope was based on that recommended as part of the Data Security and Protection (DSP) Toolkit Strengthening Assurance Guide published in 2020 by NHS Digital. As such our assessment involved the following steps:

- Obtain access to your organisation's DSP Toolkit self-assessment.
- Discuss the mandatory assertions that will be assessed with your organisation and define the evidence texts that will be examined during the assessment.
- Request and review the documentation provided in relation to evidence texts that are in scope of this assessment prior to the audit (if applicable).
- Interviewing the relevant stakeholders as directed by the organisation lead, who are responsible for each of the assertion evidence texts/self-assessment responses or people, processes and technology.
- Review the operation of key technical controls on-site using the DSP Toolkit Independent Assessment Framework as well as exercising professional judgement and knowledge of the organisation being assessed.

Selected Assertions

As based on the recommended scoping from NHS digital the selected thirteen assertions are as follows:

Area	Description
1.6	The use of personal information is subject to data protection by design and by default.
1.8	There is a clear understanding and management of the identified and significant risks to sensitive information and services
2.2	Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.

Area	Description
3.1	There has been an assessment of data security and protection training needs across the organisation.
4.2	Organisation assures good management and maintenance of identity and access control for its networks and information systems
5.1	Process reviews are held at least once per year where data security is put at risk and following data security incidents.
6.2	All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.
7.2	There is an effective test of the continuity plan and disaster recovery plan for data security incidents.
7.3	You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.
8.3	Supported systems are kept up-to-date with the latest security patches.
8.4	You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.
9.2	A penetration test has been scoped and undertaken
10.2	Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS Digital guidance.

The scope of this review included only the mandatory elements of the above selected assertions.

Appendix B: Assurance Definitions and Risk Classifications

Overall NDG Standard Assurance Rating Classification	Rating Thresholds when only 1 assertion per NDG Standard is in scope	Rating Thresholds when 2 or more assertions are in scope for each NDG Standard. Mean score (Total points divided by the number of in-scope assertions)
Substantial	1 or less	1 or less
Moderate	Greater than 1, less than 10	Greater than 1, less than 4
Limited	Greater than/equal to 10, less than 40	Greater than/equal to 4, less than 5.9
Unsatisfactory	40 and above	5.9 and above

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'

Level of deviation from the DSP Toolkit submission and assessment findings	Confidence level	Assurance level
High – 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 National Data Guardian Standards as 'Unsatisfactory' and the overall rating is 'Unsatisfactory'.	Low	Limited
Medium - 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	Moderate
Low - the organisation's self-assessment against the Toolkit does not differ / deviates only minimally from the Independent Assessment	High	Substantial

A - Summary Scoring

National Data Guardian (NDG) Standard	Number of DSP Toolkit Assertions Assessed by Independent Assessor	Number of Assertions rated **Critical** and (Weighted Risk Score)	Number of Assertions rated **High** and (Weighted Risk Score)	Number of Assertions rated **Medium** and (Weighted Risk Score)	Number of Assertions rated **Low** **and** (Weighted Risk Score)	Risk Rating Scores [total points/ no. assertions assessed]	Overall Risk Rating at the National Data Guardian Standard level	**Overall risk assessment across all 10 NDG Standards**
1. Personal Confidential Data	**2 assertions assessed out of 8 in this standard**				2 (2)		● Substantial	Substantial
2. Staff Responsibilities	**1 assertions assessed out of 1 in this standard**				1 (1)		● Substantial	
3. Training	**1 assertions assessed out of 4 in this standard**				1 (1)		● Substantial	
4. Managing Data Access	**1 assertions assessed out of 5 in this standard**				1 (1)		● Substantial	
5. Process Reviews	**1 assertions assessed out of 3 in this standard**				1 (1)		● Substantial	
6. Responding to Incidents	**1 assertions assessed out of 3 in this standard**				1 (1)		● Substantial	
7. Continuity Planning	**2 assertions assessed out of 3 in this standard**				2 (2)		● Substantial	
8. Unsupported Systems	**2 assertions assessed out of 4 in this standard**				2 (2)		● Substantial	
9. IT Protection	**1 assertions assessed out of 6 in this standard**				1 (1)		● Substantial	
10. Accountable Suppliers	**1 assertions assessed out of 5 in this standard**				1 (1)		● Substantial	
TOTAL	**13 of 42**			1 (3)	12 (12)	-	-	

B - Scoring Comparison

National Data Guardian Standard 1: Personal Confidential Data

Evidence Text Ref.	Evidence Text for Category	Health & Social Care org. DSPT Self-Assessment Rating	Independent Assessor–Evidence Text Risk Rating	Independent Assessor- Assertion Rating *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.*
1.6.1	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	Low	Low
1.6.2	There are technical controls that prevent information from being inappropriately copied or downloaded.	Met	Low	
1.6.3	There are physical controls that prevent unauthorised access to buildings and locations where personal data are stored or processed.	Met	Low	
1.6.4	Provide the overall findings of the last data protection by design audit.	Met	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	Low	
1.8.3	What are your top three data security and protection risks?	Met	Low	

National Data Guardian Standard 2: Staff Responsibilities

Evidence Text Ref.	Evidence Text for Category	Health & Social Care org. DSPT Self-Assessment Rating	Independent Assessor–Evidence Text Risk Rating	Independent Assessor- Assertion Rating *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.*
2.2.1	Is there a data protection and security induction in place for all new entrants to the organisation?	Met	Low	Low
2.2.2	Do all employment contracts contain data security requirements?	Met	Low	

National Data Guardian Standard 3: Training

Evidence Text Ref.	Evidence Text for Category	Health & Social Care org. DSPT Self-Assessment Rating	Independent Assessor–Evidence Text Risk Rating	Independent Assessor- Assertion Rating *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.*
3.1.1	Has an approved organisation-wide data security and protection training needs analysis been completed in the last twelve months?	Met	Low	Low

National Data Guardian Standard 4: Managing Data Access

Evidence Text Ref.	Evidence Text for Category	Health & Social Care org. DSPT Self-Assessment Rating	Independent Assessor–Evidence Text Risk Rating	Independent Assessor- Assertion Rating *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.*
4.2.1	When was the last audit of user accounts held?	Met	Low	Low
4.2.3	Logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity.	Met	Low	
4.2.5	Are unnecessary user accounts removed or disabled?	Met	Low	

National Data Guardian Standard 5: Process Reviews

Evidence Text Ref.	Evidence Text for Category	Health & Social Care org. DSPT Self-Assessment Rating	Independent Assessor–Evidence Text Risk Rating	Independent Assessor- Assertion Rating *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk 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	Low	Low
5.1.2	Provide summary details of process reviews held to identify and manage problem processes that cause security breaches.	Met	Low	

National Data Guardian Standard 6: Responding to Incidents

Evidence Text Ref.	Evidence Text for Category	Health & Social Care org. DSPT Self-Assessment Rating	Independent Assessor–Evidence Text Risk Rating	Independent Assessor- Assertion Rating *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.*
6.2.2	Number of alerts recorded by the antivirus/anti-malware tool in the last three months.	Met	Low	Low
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	Low	
6.2.4	Antivirus/anti-malware is kept continually up to date.	Met	Low	
6.2.5	Antivirus/anti-malware software scans files automatically upon access.	Met	Low	
6.2.6	Connections to malicious websites on the Internet are prevented.	Met	Low	

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	Low	
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	Low	
6.2.12	You have implemented spam and malware filtering, and enforce DMARC on inbound email.	Met	Low	
National Data Guardian Standard 7: Continuity Planning				
Evidence Text Ref.	**Evidence Text for Category**	**Health & Social Care org. DSPT Self-Assessment Rating**	**Independent Assessor–Evidence Text Risk Rating**	**Independent Assessor- Assertion Rating** *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.*
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	Low	Low
7.2.4	From the business continuity exercise, explain what issues and actions were documented, with names of actionees listed against each item.	Met	Low	
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	Low	
7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Met	Low	
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	Low	
7.3.5	When did you last successfully restore from backup?	Met	Low	
7.3.6	Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose	Met	Low	
National Data Guardian Standard 8: Unsupported Systems				
Evidence Text Ref.	**Evidence Text for Category**	**Health & Social Care org. DSPT Self-Assessment Rating**	**Independent Assessor–Evidence Text Risk Rating**	**Independent Assessor- Assertion Rating** *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.*
8.3.1	How do your systems receive updates and how often?	Met	Low	Low
8.3.2	How often, in days, is automatic patching typically being pushed out to remote endpoints?	Met	Low	
8.3.3	There is a documented approach to applying security updates (patches) agreed by the SIRO.	Met	Low	
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	Low	
8.4.1	Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?	Met	Low	
8.4.2	All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.	Met	Low	
National Data Guardian Standard 9: IT Protection				
Evidence Text Ref.	**Evidence Text for Category**	**Health & Social Care org. DSPT Self-Assessment Rating**	**Independent Assessor–Evidence Text Risk Rating**	**Independent Assessor- Assertion Rating** *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk 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	Low	Low
9.2.2	The date the penetration test and vulnerability scan was undertaken.	Met	Low	
National Data Guardian Standard 10: Accountable suppliers				
Evidence Text Ref.	**Evidence Text for Category**	**Health & Social Care org. DSPT Self-Assessment Rating**	**Independent Assessor–Evidence Text Risk Rating**	**Independent Assessor- Assertion Rating** *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.*
10.2.1	Your organisation ensures that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.	Met	Low	Low
10.2.2	Your organisation determines, as part of its risk assessment, whether the supplier certification is sufficient assurance.	Met	Low	
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	Low	

Assertion	Evidence ref	Evidence Text	Tool Tips	Required to meet standard (mandatory)	Exempt for NHS Mail	Exempt for Cyber Essentials PLUS	Exempt for ISO27001	Entry Level	Risk Likelihood	Risk Impact	Risk rating	Assertion Rating	Risk Points	Finding	Implications	Recommendations
The use of personal information is subject to data protection by design and by default	1.6.1	There is an approved procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements.	The procedures should be approved by the board or equivalent and aim to ensure that only the minimum necessary personal data are processed, that pseudonymisation is used where possible and that processing is transparent allowing individuals to monitor what is being done with their data.	Yes				x	20%-40%	Moderate	Low	Low	1	The Trust had in place a Data Protection Policy which set out the Trust approach to Data Protection. The Policy was agreed in June 2020 by the Information Governance Security Forum and had a review date of June 2023. Furthermore, the Trust provided a copy of the Information Governance Strategy Framework and Policy which was approved in June 2020 by the Business Performance Committee. The Strategy supported the Trust's data protection processes. We were provided a copy of the Pseudonymisation Policy which detailed the Trust's process in relation to securing personally identifiable information. The Policy was approved in August 2020 by the Information Governance Security Forum and Business Performance Committee. the review date of the policy was August 2023. The Information Governance Security Forum is chaired by the SIRO and deputy chaired by the Head of IMT. We were not provided any further evidence of how data protection and information governance featured in wider strategies.	Without appropriate controls and formalised approaches / agreements available and subject to review and risk assessment, the risk of breach increases.	1. Strengthening the inclusion of principles into wider strategies etc. that make reference to the data protection principles, and / or examples of risk management and project methodologies and policies that explicitly reference the DPIA / data protection principles would further strengthen the controls.
	1.6.2	There are technical controls that prevent information from being inappropriately copied or downloaded.	Technical controls that can support data protection include access control, encryption, computer port control, pseudonymisation techniques etc. Provide details at high level.	Yes					20%-40%	Significant	Low			During a Teams call, we were informed of the technical controls that were in operation at the Trust, this discussion included; - Data cannot be downloaded USB Drive or CD - BitLocker encryption - Email Encryption through Sophos - Pseudonymisation Policy Some of the controls were listed in the Data Protection Policy however, there was some gaps. For example, controls relating to the Web Proxy and Data Loss Prevention.	Without appropriate controls and formalised approaches / agreements available and subject to review and risk assessment, the risk of breach increases.	1. The Trust should ensure that it has documented its technical controls (such as Proxy and Data Loss Prevention controls) and these are approved by an appropriate committee of the Trust. 2. The Trust should continue to embed and mature regular assurance reviews of technical controls / associated dashboards to ensure they remain proportionate / fit for purpose.
	1.6.3	There are physical controls that prevent unauthorised access to buildings and locations where personal data are stored or processed.	Physical controls that support data protection include lockable doors, windows and cupboards, clear desk procedure, security badges, key coded locks to access secure areas etc. Provide details at high level and, if you have more than one building, summarise how compliance is assured across your organisation's sites.	Yes					20%-40%	Significant	Low			We were provided copies of SS02 - Personnel Security and Access Controls and SS06 - Physical and Environmental Security. Both documents were part of the Trust's ISMS and were approved in September 2020 and November 2020 respectively. Both documents listed the controls in operation as part of the Control Methods section. We were also provided documentation that evidenced the access controls that was in operation on the ID Pro system. We were informed that there are tests of these controls however, these are formally documented.	Without appropriate controls and formalised approaches / agreements available and subject to review and risk assessment, the risk of breach increases.	1. The Trust should develop a formal physical control testing schedule and report the outcome and any actions to a relevant group or committee.
	1.6.4	Provide the overall findings of the last data protection by design audit.	This should be in the last twelve months, covering access control, encryption, computer port control, pseudonymisation and physical controls.	Yes					<20%	Moderate	Low			We were provided the outcome of the Data Control Audit from the Radiology Department which considered the systems that the Radiology department use as part of their processes. The outcome was satisfactory and this was reported to the TIG as evidenced by minutes that was provided.	The evidence line was assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.
There is a clear understanding and management of the identified and significant risks to sensitive information and services	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?	Further guidance is available here https://www.ncsc.gov.uk/collection/risk-management-collection	Yes			x		<20%	Significant	Low	Low	1	The Trust had in place a Risk Management Policy that was approved by the Patient Safety Group and had a review date of February 2022. We were informed that the IG and IT risks were contained within the overarching Trust risk register (Datix). Risks are monitored through the Information Governance and Security Forum (now TIG) and reported on a monthly basis to the Corporate Governance Risk Meeting on a Monthly basis.	The evidence line was assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The Trust should review its risk management processes and ensure where applicable third party risks identified through DPIAs and due diligence checks are linked to the corporate risk framework.
	1.8.3	What are your top three data security and protection risks?	Record at a heading level	Yes					20%-40%	Significant	Low			The policy stated that risks are scored on the likelihood by impact methodology using 5X5 scoring. The top 3 IT/IG risks were identified as follows; - Data Breach - Cyber Security - Security for Hardware and Clinical Devices. Each was rated at 4 at the time of the review. 2 of the risks had not been reviewed at their review date of 28/03/2021. The Information Security Management Forum were responsible for assessing these risks, the membership included the SIRO, DPO and Head of IT and IT Security Manager.	Without an appropriately detailed remediation plan in place, the risk of one of these issues being realised increases and could result in fines, non-compliance and / or reputational damage.	1. The Trust should ensure it continues to review its top three risks prior to submission with consideration of any new risks posed. 2. The residual risk should be considered and, appropriately detailed remediation plans / risk tolerances acknowledged, recorded and accepted.
Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.	2.2.1	Is there a data protection and security induction in place for all new entrants to the organisation?	The induction can be delivered face to face or digitally. Records are maintained and the induction is reviewed on a regular basis to ensure its effectiveness.	Yes			x		<20%	Moderate	Low	Low	1	We were provided an ESR report from December 2020 which showed all staff that was appointed had undertaken their mandatory training which included Data Security Awareness. Furthermore, the Trust provided a copy of their Information Governance Corporate Induction presentation which is used as part of the induction process at the Trust. Review of the materials confirmed it contained key principles of IG at the Trust.	The evidence line was assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The Trust should continue to ensure all new starters complete their induction training in line with stated policy.
	2.2.2	Do all employment contracts contain data security requirements?	Please provide any explanatory text in the comments box	Yes			x	x	<20%	Moderate	Low			The Trust provided a copy of its standard contract of employment. Review of the contract confirmed that the confidentiality and access to information section contained the included the necessary data protection clauses as required.	The evidence line were assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.
There has been an assessment of data security and protection training needs across the organisation.	3.1.1	Has an approved organisation-wide data security and protection training needs analysis been completed in the last twelve months?	This is an assessment of data security and protection training and development needs for all your staff including Board Members. Approved by your SIRO or equivalent.	Yes			x		<20%	Moderate	Low	Low	1	The Trust provided a copy of the 2020-21 Training Needs Analysis for the Information Governance team which covered the period April 2020 to March 2021. The TNA was approved by the ISGF in October 2020 which included attendance by the SIRO. Review of the TNA confirmed it included training needs for all staff in relation to mandatory IG training and also for specialist staff such as the IG manager/officers.	The evidence line were assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.

Assertion	Evidence ref	Evidence Text	Tool Tips	Required to meet standard (mandatory)	Exempt for NHS Mail	Exempt for Cyber Essentials PLUS	Exempt for ISO27001	Entry Level	Risk Likelihood	Risk Impact	Risk rating	Assertion Rating	Risk Points	Finding	Implications	Recommendations
Organisation assures good management and maintenance of identity and access control for it's networks and information systems.	4.2.1	When was the last audit of user accounts held?	An audit of staff accounts from your organisation, to make sure there aren't any inappropriate access permissions. Record the date when the last user audit was held. This should be completed annually as a minimum	Yes			x		20% - 40%	Significant	Low	Low	1	During a Teams call, we were shown evidence that the IT Team receive a daily report for AD that includes all accounts that haven't been used in the previous 30 days. We requested a leavers list from ESR for April 2021 which included 5 users, we were also provided an AD listing in May 2021. Comparison of the two documents provided found that the user accounts for 4 of the users had been disabled with the remaining user still active. The user account belonged to a senior staff member, we were informed by the Head of IT that they were aware that the user account had remained open as it was deemed that there was business critical emails that the former employee's PA was picking up, sorting and forwarding to the most appropriate team member although documented confirmation of this was not provided. IT did not provide detail on how they were assured the leaver was not able to access the system or of any mitigations that had been applied to the account to maintain security. There was also no evidence provided of user account reviews for individual systems not linked to AD or domain admins.	Inappropriate user accounts or associated inappropriate privileges granted, increase the risk of malicious or accident damage to systems or data breaches.	1. The Trust should gain assurance that the user identified does not continue to have access to their user account. 2. The IT Team should consider alternative arrangements until a new user is appointed to the identified user's role. 3. The requirement to keep a leaver's account open should be formally risk assessed with approval sought from the SIRO/member of the Executive team. 4. The Trust should ensure user account audits are completed areas and systems other than AD user accounts
	4.2.3	Logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity.		Yes					20%-40%	Significant	Low			We were provided the SS11 - Monitoring and Auditing (Log Retention Control) document that was approved by the ISMF in August 2020. The documentation confirmed what information would be logged, such as log on and log off times. This also included information such as VIP markers. The document confirmed that logs would be maintained however, it was noted that the document itself did not confirm how long logs were retained. We noted the document referenced other documentation however, we were not provided this at the time of the review. It was confirmed that logs are maintained for at least 6 months and at the time of the review, the Technical Infrastructure Group (TIG) was reviewing to confirm logs had been maintained as per the documentation. At the time of the review, this task had not been completed by the TIG. We were provided screenshots of the SIEM which showed evidence of the logs being retained by the Trust.	Inappropriate user accounts or associated inappropriate privileges granted, increase the risk of malicious or accident damage to systems or data breaches.	1. The Trust should review the SS11 document and consider including how long logs are retained by the Trust. 2. The Trust should continue with its review to ensure logs are being kept for the appropriate timeframe.
	4.2.5	Are unnecessary user accounts removed or disabled?	Former employees', guest and other unnecessary accounts are routinely and promptly removed or disabled from internal workstations, Active Directory domains and other user directories. Privileged user access is also removed when no longer required or appropriate.	Yes		x			20% - 40%	Significant	Low			We requested a leavers list from ESR for April 2021 which included 5 users, we were also provided an AD listing in May 2021. Comparison of the two documents provided found that the user accounts for 4 of the users had been disabled with the remaining user still active. The user account belonged to a senior staff member, we were informed by the Head of IT that they were aware that the user account had remained open as it was deemed that there was business critical emails that the former employee's PA was picking up, sorting and forwarding to the most appropriate team member although documented confirmation of this was not provided. IT did not provide detail on how they were assured the leaver was not able to access the system or of any mitigations that had been applied to the account to maintain security.	Inappropriate user accounts or associated inappropriate privileges granted, increase the risk of malicious or accident damage to systems or data breaches.	1. The Trust should gain assurance that the user identified does not continue to have access to their user account. 2. The IT Team should consider alternative arrangements until a new user is appointed to the identified user's role. 3. The requirement to keep a leaver's account open should be formally risk assessed with approval sought from the SIRO/member of the Executive team.
Process reviews are held at least once per year where data security is put at risk and following data security incidents.	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.	Explain how any incident response and management tests findings have informed the immediate future technical protection and remediated any systemic vulnerabilities of the system or service, to ensure identified issues cannot arise in the same way again.	Yes			x		20% - 40%	Significant	Low	Low	1	We were provided a copy of the Trust's SS08 - Incident and Change Management document as part of the ISMS. The document had been reviewed in August 2020.Review of the documentation found that it did not clearly document the Trust's Incident RCA process. The document did however document the controls and process of management of IS incidents. We were provided evidence that RCAs are reported to the ISMS Risk Group where there were documented controls and lessons learnt. Furthermore, IG incidents are discussed at the IGSF, where we had received evidence that controls and lessons learnt are presented. The Trust provided evidence that the SIRO report is presented at the Business Performance Committee. The report was provided on a monthly basis and could be tracked back to the incidents reported in the ISMS and IGSF groups.	Without correctly completed Root Cause Analysis documentation, identifying lessons learnt for a range of categories, risk of future occurrences increases	1. The Trust should review the SS08 - Incident and Change Management document and consider including the RCA process for data security incidents.
	5.1.2	Provide summary details of process reviews held to identify and manage problem processes that cause security breaches.	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.	Yes			x		<20%	Significant	Low			The IS Management Policy was provided and includes details of the post incident review process that is in operation at the Trust. We were informed that the Trust had documented a post incident review in relation to a Cisco incident that had occurred in February 2021. We were shown the details of the review during a Teams call with the Trust and the reviewed documentation contained conclusion and recommendations. We were not provided any minutes to verify the review/action points had been reported to ISGF.	Without correctly completed Root Cause Analysis documentation, identifying lessons learnt for a range of categories, risk of future occurrences increases	1. The Trust should ensure that they document the monitoring of actions at the appropriate committee.
All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.	6.2.2	Number of alerts recorded by the antivirus/anti-malware tool in the last three months.	Your antivirus/anti-malware software should record alerts of any potential threats to your system. Provide the number which have been recorded over the last three months. You may need to speak to your IT Supplier to learn how to view this information.	Yes		x			20%-40%	Significant	Low			We were shown the Trust's AV solution, TrendMicro, that was used for scanning of potentially malicious files that enter the Trust's IT estate. We were shown evidence of alerts from the system either via download or via emails which are blocked and quarantined. We were also shown evidence that if files cannot be scanned by TrendMicro then these are blocked from the network. The Trust provided the Vulnerability Management Procedure that included some details of the anti-virus process however, this could be strengthened to include how the Trust manages alerts. The procedure had not been updated since February 2019. The Trust's toolkit included alerts for the previous 3 months which totalled 1 alert in March 2021.	Without appropriate documented controls and processes in relation to anti-virus, the risk of malware infecting the Trust's IT systems is increased.	1. The Trust should review its Vulnerability Management Procedure to ensure its up to date and consider increasing the documentation of anti-virus within the documentation.
	6.2.3	Has antivirus/anti-malware software been installed on all computers that are connected to or capable of connecting to the Internet?	This applies to: application servers; desktop computers; laptop computers, tablets and mobile devices running windows desktop operating systems. Please include the name of your anti-virus product in the comments.	Yes		x	x		20%-40%	Significant	Low			Testing was undertaken on a sample of 5 servers and 5 endpoints. Each was found to have the AV software included on the devices tested. It was noted that coverage of AV across the Trust's IT Estate was not included for reporting within the Information Management Security Forum or Technical Infrastructure Group We were provided evidence that the Trust's AV solution is part of the Trust's base build for devices.	Devices without adequate anti-virus are susceptible to malware attacks.	1. The Trust should provide regular updates to the ISMF or relevant group/committee of the coverage of AV across the IT estate, for assurance. 2. Where devices are found not to have AV, this should be reported to the IMSF (or equivalent) and action plans should be monitored to remediate the issue.
	6.2.4	Antivirus/anti-malware is kept continually up to date.	Provide an explanation of how this is achieved. This could be through automatic update, central deployment, ATP etc.	Yes					<20%	Significant	Low			The Trust demonstrated via Teams call the AV settings that were applied within TrendMicro, the settings included; - Update of definitions every hour - Definitions would be pushed out to devices every hour - updates to TrendMicro were set to update on a monthly basis.	The evidence line was assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.

Assertion	Evidence ref	Evidence Text	Tool Tips	Required to meet standard (mandatory)	Exempt for NHS Mail	Exempt for Cyber Essentials PLUS	Exempt for ISO27001	Entry Level	Risk Likelihood	Risk Impact	Risk rating	Assertion Rating	Risk Points	Finding	Implications	Recommendations
	6.2.5	Antivirus/anti-malware software scans files automatically upon access.	This includes when files are downloaded and opened, and when they are accessed from a network folder.	Yes					<20%	Significant	Low	Low	1	As per 6.2.5, the AV software was configured to scan all potentially malicious files prior to download. This were evidenced on a Teams call. We were also shown evidence of the latest weekly scan for workstations and the real time scan solution using InteliScan Furthermore, we were shown evidence of the logs retained in regards to scanned files.	The evidence line was assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.
	6.2.6	Connections to malicious websites on the Internet are prevented.	This applies to all corporate devices. It may be achieved by one or more of the following using a web proxy, antivirus/anti-malware, browser tools. Protective DNS services, blacklisting or other mechanisms.	Yes					<20%	Significant	Low			The Trust has in place web proxy controls that prevent connections to malicious websites. We were shown the definitions whilst on a Teams call. Furthermore, we were shown the latest web proxy alerts for the Trust. We were not provided documented evidence of how the alerts for web proxy are managed by the Trust's IT team.	Without appropriate documented controls and processes in relation to anti-virus, the risk of malware infecting the Trust's IT systems is increased.	1. The Trust should formally document its process/procedure in relation to management of web proxy / anti-virus alerts.
	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.	This applies to email, Servers, desktop computers, laptop computers, tablets and mobile phones.	Yes					<20%	Significant	Low			We were provided the Control Software Library which documented the software that had been approved by the IT team and the staff groups that should have access to them. We were informed by the Deputy Head of IMT that there hadn't been any requests for software installations above this during the year. Local Admin rights should be requested through the IT Service Desk and agreed as appropriate by the IT team. The Deputy Head of IMT demonstrated that there was no local admins during a teams call.	The evidence line was assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.
	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.	This applies to email systems	Yes	x				<20%	Moderate	Low			The Trust provided evidence of DKIM, DMARC and SPF policies being enabled within the systems of the Trust.	The evidence line was assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.
	6.2.12	You have implemented spam and malware filtering, and enforce DMARC on inbound email.	This applies to email systems and should include the name of the filtering product.	Yes	x				<20%	Moderate	Low			The Trust provided evidence of DKIM, DMARC and SPF policies being enabled within the systems of the Trust. We were shown an example of an email that was quarantined in TrendMicro during a Teams call with the Senior Infrastructure Engineer.	The evidence line was assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.
There is an effective test of the continuity plan and disaster recovery plan for data security incidents.	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.	Exercise scenarios should be based on incidents experienced by your and other organisations, or are composed using threat intelligence. This should be in the last twelve months with active board and business representation.	Yes			x		20%-40%	Significant	Low	Low	1	The Trust undertook testing on its Information Security Management System on 26th May 2021. We were provided the details of the exercises undertaken as part of the sessions and the log of actions following the test. We were not provided evidence that the actions had been reported to a relevant group/committee for oversight. We were informed that the SIRO attended the session however, the attendance sheet did not contain the signature of the SIRO.	Untested and / or unmaintained plans can cause prolonged disruption and delays in recover should an event occur.	1. The Trust should ensure that future exercises include the SIRO or a deputy/board level executive and be able to evidence their attendance.
	7.2.4	From the business continuity exercise, explain what issues and actions were documented, with names of actionees listed against each item.	Each action should have an owner and timescale.	Yes			x		20%-40%	Significant	Low			As per 7.2.1, action plans for each exercise where created with action owners and expected completion dates. The Trust did not provide evidence that these had been reported as part of the governance structure.	Untested and / or unmaintained plans can cause prolonged disruption and delays in recover should an event occur.	1. The Trust should formalise their action plans as part of the risk management framework. work.
You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.	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.	Advice is available form NHS Digital or a cyber incident response company.	Yes					<20%	Significant	Low	Low	1	We were provided a copy of the Trust's IT Business Continuity and Disaster Recovery standard which had been approved in October 2020 by the Information Security Management Forum (ISMF). Review of the standard confirmed that third party resource had been identified and contact details had been included in the standard. This included supplier contracts and specialist support from NHS Digital.	The evidence line was assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.
	7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Contacts include phone number as well as email.	Yes			x		20%-40%	Significant	Low			The Trust maintains hard copies of the emergency contact list in an IT Safe. We were not informed of the frequency of review. Due to the remote nature of the review, we have not been able to verify the hard copies exist in the safe. The Deputy Head of IMT confirmed that the Trust uses MS Teams to store emergency contacts as they system should be operational regardless of the status of the Trust's IT Estate. We were provided screenshots of the documentation and whom had access to the files which included senior members of the IT team.	Incident response may be delayed with prolonged downtime if emergency contacts are unknown, out of date or inaccessible.	1. The Trust should ensure all copies of emergency contacts are frequently updated and include relevant areas/contacts in the event of an emergency. For IT, this could include third party system suppliers and support.
	7.3.4	Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.	Provide evidence that your backup, testing and review process is effective.	Yes		x	x		20%-40%	Significant	Low			We were provided a recently updated document showing the backup environment of the Trust. This included details of the backup to tapes in operation for critical systems. It was advised: Online backup copies are located in separate physical (building) location to the source data onto network attached backup media. The backup servers have been isolated from the direct access VPN client subnet for added protection. Backup Servers are protected by AntiVirus, IPS & IDS software and appropriate NTFS permissions. We were provided an example of backup restore that had been undertaken during 9th May 2021. Furthermore, during a teams call with the Senior Infrastructure Engineer, we were shown evidence that the organisation tests the backups. This was shown by a recent test being shown during the call. The Trust has a report that shows the recovery point status of each server within the Trust's IT infrastructure. Discussions with the Trust confirmed that Recovery Point Objectives had not been agreed with IAOs.	Timely backup data could be impacted without agreed timeframes / regular testing.	1. The Trust should review / confirm its RTO and RPO provisions, especially for critical systems, with the IOAs to ensure they continue to meet business needs.
	7.3.5	When did you last successfully restore from backup?	Backups should be tested frequently. The example provided may relate to a live or test environment.	Yes		x	x		<20%	Significant	Low			As per 7.3.4 - we were provided an example restore from 9th May 2021.	Timely restores could be impacted without agreed timeframes / regular testing.	1. The Trust should formalise a regular schedule for testing. 2. Any residual risks should continue to be monitored via the risk register.
	7.3.6	Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose	Cloud synching services, such as OneDrive, SharePoint or Google Drive, should not be used as your only backup and stored backup should not be permanently connected to your network. Further guidance at https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world.	Yes					20% - 40%	Significant	Low			We were provided a Secure Backup review that was undertaken by MTI and reported in April 2021, the main issues raised were; • Veeam provides no offline/immutable copies • DPM provides no offline/immutable or 2nd copies • Although the backup solution is tied into Active Directory, a Privileged Account Management (PAM) system is not in place to prevent authentication-based attacks from being successful in compromising the backup server(s) • No segregation is in place to limit connectivity to the backup administrative interface • There is not a separate backup network We were not provided any evidence that the actions had been reported to a suitable committee or group or any agreement of an action plan to remediate the issues identified however it was advised that the findings are currently being evaluated by the Trust Confirmation was provided of an offline backup solution for critical systems (EPR, PAS, Pathology) which are backed up to tape. Tapes are kept in a locked cupboard in an IT storeroom on the Trust site but within a different building to the one hosting the data centre. This solution has been recently reimplemented and should be risk assessed to ensure this provides appropriate protection for the Trust in the event of a ransomware attack.	Without backups being regularly replicated to offline storage in line with agreed policy, the risk from ransomware increases and could result in service disruption and impact patient care.	1. The actions raised by MTI should be formally reported to an appropriate committee/group. 2. The tape back up solution should be formally risk assessed to ensure it meets organisational needs. 2. The Trust should consider managing the risks via the Risk Management Process.

Assertion	Evidence ref	Evidence Text	Tool Tips	Required to meet standard (mandatory)	Exempt for NHS Mail	Exempt for Cyber Essentials PLUS	Exempt for ISO27001	Entry Level	Risk Likelihood	Risk Impact	Risk rating	Assertion Rating	Risk Points	Finding	Implications	Recommendations
Supported systems are kept up-to-date with the latest security patches.	8.3.1	How do your systems receive updates and how often?	This is your strategy for system updates. You may need your IT supplier/s to assist with this.	Yes					20% - 40%	Significant	Low	Low	1	We were provided documentation to support the Trust's endpoint and server patching processes this was included within SS07 - Cyber Security which had been approved in July 2020. The Trust also provided the Vulnerability Management Procedure that confirmed the Trust patches systems on a monthly basis. The procedure had not been updated since February 2019. Testing was undertaken on a sample of 5 endpoints and 5 servers identified from a listing provided by the Trust. Testing on the 5 servers found that each had been patched within 30 days at the time of the test. Testing on a sample of 5 endpoints (mixture of desktops and laptops) found that 4 had been updated within the previous month. The remaining endpoint was last updated in April 2021 however, the Trust provided evidence that the asset software had not been correctly applied. It was noted that the endpoint had not been online recently to receive an update and therefore, it was suspected it had been retrieved for a rebuild. It was noted that the Trust deploys virtual patching to devices that run operating systems that are out of support through the Trend Micro software. Whilst it does represent some risk mitigation, the Trust should endeavour to remove operating systems from the estate that are no longer support.	Unpatched systems are vulnerable to known exploits that can cause instance including service disruption, data loss, or breach, etc. not just for the system in question but also the organisation interconnected infrastructure	1. The Trust should develop a plan to remove out of support operating systems so that the reliance on virtual patching is removed.
	8.3.2	How often, in days, is automatic patching typically being pushed out to remote endpoints?	Remote endpoints being those devices or computers that are not on the core network (such as home or mobile workers). Provide the usual number of days between one wave of remote patching and the next.	Yes					<20%	Moderate	Low			Testing on a sample of 5 endpoints (mixture of desktops and laptops) found that 4 had been updated within the previous month. The remaining endpoint was last updated in April 2021 however, the Trust provided evidence that the asset software had not been correctly applied. It was noted that the endpoint had not been online recently to receive an update and therefore, it was suspected it had been retrieved for a rebuild. During the testing on a teams call, the Senior Infrastructure Engineer showed that some of the devices that were not on the Trust site and should still be receiving updates.	The evidence line was assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.
	8.3.3	There is a documented approach to applying security updates (patches) agreed by the SIRO.	Provide details in the comments box. This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers, desktop computers, laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services.	Yes		x			<20%	Moderate	Low			The Trust provided the Vulnerability Management Procedure that included details of the Trust's Patch Management Procedure including CareCERTs. The procedure had not been updated since February 2019. The 3 latest high risk vulnerabilities published by NHS digital (commonly known as CareCERTs) had either been resolved by the Trust or were not an applicable vulnerability to the Trust. Each CareCERT in our sample was resolved within 14 days or in one case, not required at the Trust. This was evidenced through the NHS Digital portal.	The evidence line were assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.
	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.	Provide summary details in the comments box. Documentation should be held locally for all security patches. This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers, desktop computers, laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services. Devices that are unable to be patched should be captured under 8.1.3. Devices that are standalone or air-gapped should be captured under 9.6.10.	Yes		x			<20%	Significant	Low			We were informed that there had been no high/critical risk security patches that had not been remediated within the agreed timeframes. Therefore, there were no occasions where the SIRO needed to accept the Risk. We were provided reports received by the Information Security Management Forum which confirmed that each high/critical risk vulnerability had been patched within 14 days or deemed not applicable to the Trust.	The evidence line was assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.
You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.	8.4.1	Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?	Explain at a summary level. Where it is not possible to apply these measures, explain any mitigations (such as logical separation).	Yes					<20%	Significant	Low	Low	1	Technical controls in place as per 1.6. The Trust uses TrendMicro as its AV solution as per 6.2 As per 8.3 - Yes all infrastructure protected through secure configuration & patching in a timely manner. As per 8.3 - Patches are pushed out as per routine patching "Patch Tuesday" as a minimum once a month. CareCERTs due to their high level nature are remediated immediately. We were informed that the Trust Cyber Security Manager is the chair of the Northwest WARP where related issues are discussed. We were also provided the Trust ISO27001 accreditation which had been completed in October 2020 by Alcumus.	The evidence line was assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.
	8.4.2	All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.	Covers software running on computers that are connected to or capable of connecting to the Internet. Unsupported software should be covered under 9.6.10.	Yes					20%-40%	Significant	Low			We reviewed the Trust's Software Asset Register on a call with the Senior Infrastructure Engineer. There were some instances of servers running Windows Server 2008 however, we reviewed evidence of an action plan to remediate this which was reported to the Information Security Management Forum. We reviewed a sample of 3 software assets that had reached end of support. Each of these had been raised on the risk register and had been agreed and monitoring by the ISMF. These meetings included the SIRO	Unpatched systems are vulnerable to known exploits that can cause incidents including service disruption, data loss, or breach, etc. not just for the system in question but also the organisation and interconnected infrastructure.	1. The Trust should continue to monitor its IT Estate and remediate the Windows 2008 Servers as soon as possible.
A penetration test has been scoped and undertaken	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.	Please include the scope and redact any elements of the results that are sensitive.	Yes		x			20%-40%	Significant	Low	Low	1	The Trust provided a copy of the Internal Vulnerability Assessment which was conducted in May 2021 by Sapphire. During a teams call, we were shown evidence that the scope for the review included domain passwords and vulnerability scanning. We were not provided evidence that the scope of the review was approved by the SIRO. Also, the evidence provided did not show the outcome of the review and we were not able to establish if actions had arisen from the review and had been reported to an appropriate group or committee. Furthermore, the Trust also provided an example of a Cyber Security Review and Gap Analysis undertaken by MIAA in 2020-21. The scope of the review included testing on IT Security Controls in operation by the Trust.	Untested controls increase instances of service disruption, data loss, or breach, etc.	1. For future penetration and vulnerability scans, the SIRO should approve the scope of the review. 2. Where actions have arisen, the Trust should report these to an appropriate group/committee who will oversee completion of the actions.
	9.2.2	The date the penetration test and vulnerability scan was undertaken.	This should be in the last twelve months.	Yes		x			<20%	Significant	Low			The penetration testing and vulnerability scan was completed by Sapphire on the 20th May 2021.	Untested controls increase instances of service disruption, data loss, or breach, etc.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.
Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS Digital guidance.	10.2.1	Your organisation ensures that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.	For more information see the '2017/18 Data Security Protection Requirements guidance' (https://improvement.nhs.uk/documents/2643/17-18_DSPR_Statement_of_Requirements_-_QUESTIONS_11April.pdf).	Yes					20%-40%	Significant	Low			The Trust provided a copy of the Information Governance Strategy Framework and Policy which included the process for supplier certifications and assessments to meet Data Security Standard 10. This included; - Governance Requirements in third party contracts - Governance requirements in outsourcing requirements - Contracts of third party contractors. Discussions with the Procurement team confirmed that most contracts are appointed from an NHS Framework which requires certain certifications to be part of and to maintain membership of the framework. Where there isn't, the Trust has a Procurement and Tendering Policy which details the Trust's processes however, we were not provided a copy of this. We undertook testing on a sample of 3 contracts, each had the relevant clauses, responsibilities of the supplier and the certifications that was required as part of the contract. The contracts reviewed within the sample included; - Silverlink PAS - HealthRoster - G-Cloud We were not provided evidence that supplier certifications are monitored following the onboarding of the supplier.	The Trust as the accountable organisation would be responsible for any issues experienced by processes undertaken by suppliers on their behalf and as such it is essential that appropriate checks are in place and repeated periodically.	1. The Trust should develop a contract monitoring process to allow for certifications to be monitored during the full length of the contract.

Assertion	Evidence ref	Evidence Text	Tool Tips	Required to meet standard (mandatory)	Exempt for NHS Mail	Exempt for Cyber Essentials PLUS	Exempt for ISO27001	Entry Level	Risk Likelihood	Risk Impact	Risk rating	Assertion Rating	Risk Points	Finding	Implications	Recommendations
	10.2.2	Your organisation determines, as part of its risk assessment, whether the supplier certification is sufficient assurance.	Suppliers may include other health and care organisations. For more information see the '2017/18 Data Security Protection Requirements guidance' (https://improvement.nhs.uk/documents/2643/17-18_DSPR_Statement_of_Requirements_-_QUESTIONS_11April.pdf).	Yes					<20%	Significant	Low	Low	1	We were shown evidence on a teams call of a contract that had been appointed off framework that had been assessed in line with the Information Governance Strategy Framework and Policy. It was noted that the 3 contracts selected for testing had been appointed via a framework.	The evidence line was assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.
	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.		Yes			x		<20%	Significant	Low			As per 10.2.1 - G-Cloud is a supplier delivering their service via cloud software. The roles and responsibilities are included within the contract.	The evidence line was assessed, no issues were identified however there always remains a residual risk associated with any processing activity.	1. The residual risk should be considered and, if appropriate be acknowledged, recorded and accepted.

D - Scoring Guide - Impact

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 the organisation*.*
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 a 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.

E - Scoring Guide - Likelihood

Likelihood rating	Assessment rationale
>80%	> 80% likely to happen in the next 12 months
60% - 80%	60% - 80% likely to happen in the next 12 months
40% - 60%	40% - 60% likely to happen in the next 12 months
20% - 40%	20% - 40% likely to happen in the next 12 months
< 20%	Low likelihood to happen in the next 12 months

F - Scoring Guide - Risk Rating

	Impact rating				
Likelihood rating (in next 12 months)	Critical	Significant	Moderate	Minor	Very Low
>80%	Critical	High	Medium	Low	Low
60% - 80%	High	Medium	Medium	Low	Low
40% - 60%	Medium	Medium	Low	Low	Low
20% - 40%	Medium	Low	Low	Low	Not reportable
< 20%	Low	Low	Low	Not reportable	Not reportable

Rating	Points for each Assertion
Critical	40
High	10
Medium	3
Low	1