Healthier Communities, Outstanding Care

NHS Sherwood Forest Hospitals NHS Foundation Trust

Board of Directors

Subject:	Data Security Protection Toolkit	**Date:** 2nd April 2020
Prepared By:	Jacquie Widdowson, Information Governance Manager & Data Protection Officer	
Approved By:	Shirley Higginbotham, Director of Corporate Affairs , Paul Robinson,	
Presented By:	Chief Financial Officer & SIRO	

Purpose

To provide assurance to Board of Directors on the compliance with the Data Security Protect Toolkit.	**Approval**	
	Assurance	x
	Update	
	Consider	

Strategic Objectives

To provide outstanding care	To promote and support health and wellbeing	To maximise the potential of our workforce	To continuously learn and improve	To achieve better value
x		x	x	x

Overall Level of Assurance

	Significant	Sufficient	Limited	None
		x		

Risks/Issues			**Risks/Issues**	
Financial	IG Breaches can result in significant financial penalties			
Patient Impact	IG Breaches can result in the disclosure of patient sensitive information			
Staff Impact	IG Breaches can result in the disclosure of staff sensitive information, impact on delivering care if patient information is not available or incorrect			
Services	Ensure information is available to deliver patient care			
Reputational	Potential negative impact to trust breaches			

Committees/groups where this item has been presented before

Audit Committee 19th March 2019, who approved submission of the Toolkit

Executive Summary

This report provides the Board of Directors with an overview of the Trust's compliance with the Information Governance (IG) and security agenda both nationally and locally.

The 2019/20 Annual SIRO report is included at Appendix A.

As of 11th March 2020 we are showing 95.17% of staff completing mandatory IG Training, the highest % achieved to date this year. The IG Team has been emailing individuals on an ongoing basis when their training is due to expire. This has had a positive impact on the number of employees renewing their IG Training.

Five incidents have been escalated as level 2 incidents which required reporting during 2019/20–to the Information Commissioners Office (ICO). None has resulted in action from the regulators as the Trust provided appropriate assurance.

Work continues to raise the profile of information governance across a variety of mediums to ensure that incidents and lessons learned are raised to the attention of all employees across the Trust.

APPENDIX A

2019/20 Annual Senior Information Risk Owner Report

Purpose of the Report

To document the Trust's compliance with legislative and regulatory requirements relating to the handling of information, including compliance with the Freedom of Information Act 2000, current Data Protection Act 2018 and the General Data Protection Regulations.
To document the Trust's compliance with the Data Protection & Security Toolkit and provide assurance of progress in relation to the requirements which are mandated for completion.
To detail any Serious Incidents Requiring Investigation (SIRI) during the year, relating to any losses of personal data or breaches of confidentiality.
To outline the direction of information governance work during 2019/20 and how it aligns with the strategic business goals of Sherwood Forest Hospitals NHS Foundation Trust.

Assurance Framework

The Information Governance Committee meets on a bi- monthly basis to assess risks to security and integrity of information and management of confidential information. The Committee monitors the completion of the Data Protection Security Toolkit submission, data flow mapping, and information asset registers and also ensures the Trust has effective policies, processes and management arrangements in place.

Final preparations for submission have been completed with 116 of the 116 Mandatory evidence items completed. There have been an additional 16 mandatory requirements added to the DSPT for 2019/20, these mainly focus on IT security.

Data Flow Mapping

The SIRO is responsible for the development and implementation of the organisation's Information Risk agenda. During 2019/20 the Trust has undertaken an annual review of information flow mapping to ensure we are assured information flows into and out of the Trust are identified, risk assessed and addressed. This is then expanded to ensure that we have assurance all information is stored securely and appropriately and any partners in delivery of either shared care or information storage achieve the same high levels of information governance assurance. A review of controls audit has been conducted and it has identified some weaknesses within the flow maps, an action plan has been developed to address the weaknesses and strengthen the security of the data flows.

Information flows have been received 2019/20 from the following departments:

Audiology
Chaplaincy
Day Case
Estates & Facilities
HR
Infection Prevention and Control Department
Information Services
Integrated Sexual Health Services
Management Secretaries
Medway
MEMD
NHIS
Pathology
Pharmacy
Programme Management Office
Risk
Research & Development
Stroke
Therapy
Training & Development
Trust Headquarters

Outstanding Data Flow Maps

Accident & Emergency
Cancer Services
Cardiology
Communications
Dermatology
Diabetes
Finance
Patient Services
Pre-op
Radiology
Respiratory
Women & Children

All outstanding data flow maps will be chased and support given to complete by 31st March 2020.

Review of Audit Controls

An audit was undertaken as a requirement of the DSPT, which required the Trust to review the implementation of technical controls. The controls audited included, psuedomymisation, anonymisation, access controls, encryption, computer ports and physical controls. Documents used to conduct the audit mainly consisted of the data flow maps, Information Asset Registers and Data Protection Impact Assessments. The majority of the information required is captured in the documents already in use. However, several key themes emerged, there was often duplication in the information recorded and many columns in the registers are unpopulated. It is further evident that those completing the documents have little guidance to refer to in order to support them when completing.

A wider piece of work will be undertaken to set up a regular program of auditing with the IAO's to fully understand the access and security of the information we hold.

Several keys actions have been developed into an action plan for consideration by the IG Committee who will monitor this.

Serious Incidents Requiring Investigation (SIRI)

As part of the Annual Governance Statement, the organisation is required to report on any Serious Incidents (SIRI's) or Cyber Incidents which are notified on the Data Security & Protection Toolkit reported through to either the ICO or NHS Digital.

To date there have been 5 incidents reported. The Trust has had no further action from the regulators after investigation.

Risk Management and Assurance

The SIRO is responsible for the development and implementation of the organisation's Information Risk agenda. During 2019/20 the Trust has undertaken a fresh review of information flow mapping to ensure we are assured that information flows into and out of the Trust are identified, risk assessed and addressed. This is then expanded to ensure assurance all information is stored securely and appropriately and any partners in delivery of either shared care or information storage achieve the same high levels of information governance assurance.

The SIRO and Caldicott Guardian received formal training on their statutory responsibilities during 2019/2020 in order to ensure refresh of skills and awareness of legislative changes.

The Data Protection Officer (DPO) continues to work with strengthening our relationship with the ICO and NHS Digital, by engaging in and taking part in pilot audits. This year the Trust taken part in a pilot audit by NHS Digital and 360 Assurance which involved taking a more in depth look at our process and practices aligned to the DSPT. The report provided the Trust with Significant Assurance.

The Trust is also engaging in the Cyber Operational Readiness Support (CORS) Assessment with PA consulting and NHS Digital. The assessment will support the Trust in developing a gap analysis and remediation plan to achieve the Cyber Essential plus certification by 2021.

Freedom of Information (FOI)

During 2019/20 the Trust processed a total of 475 FOI requests. This function is managed by the Information Governance Team and the activity is demonstrated in the table below.

Total	Breached timeframe of 20 days	Escalated to ICO
475	79	1

Any breaches in the 20 working day statutory response timeframe are due to complex requests that require input from multiple teams or due to an issue with a gap in the process, which has now been addressed and will ensure where possible full compliance.

Of the 475 requests, 396 are currently completed, 5 on hold waiting further information and 26 still in progress. Of the 475 requests completed 396 have been completed within 20 days which shows a compliance rate of 83%.

The 1 FOI that was escalated to the ICO, referred to individuals genetic data which could have potentially been identifiable due to the geographical location. The ICO supported the Trust with the response to the requestor and no action was taken.

Subject Access Requests

The Trust has received 2988 requests for access to patient records. The majority of cases are processed in line with national guidance which is exemplary given some of these cases represent hundreds of pages of information and require methodical attention to detail to ensure information is released appropriately. There have been no complaints to the Information Commissioner – any requests for review of content of records by patients have been handled locally and achieved satisfactory resolution for patients. The access to records team have seen a 18.33 % increase in requests from January 2017 to January 2020, and are currently monitoring whether this is due to the changes in the DPA 2018 or attributable to other care providers as we work to a more integrated service. Appendix C provides a brief explanation to those which have gone over the statutory timescale.

April 2018 to March X 2019 Total	Completed < 21 days	Completed 21-30 days	Completed > 30 days
2988	KM -2097 NWK -456 IG-18	KM-361 NWK –43 IG 6	KM –0 NWK -6 IG -1

APPENDIX B

Horizon Scanning 2020/21

The information governance landscape is changing at an alarming rate, with ever changing privacy regulations and information security challenges to protect the Trust data.

The lines between information governance and data/ IT governance continue to overlap and as a Trust we need to develop a strong information/ data governance model to adapt to new emerging technologies, environmental and social governance. We are seeing social governance changes in the form of integrated care services (ICS) which will enable us to achieve better outcomes for patients and their carers. With this there is the need to share more information at greater speed and the Trust also needs to develop a governance model to support this.

Data breaches will remain a cybersecurity concern, as data remains valuable to criminals. The Trust will need to continue to strengthen its data privacy and security controls.

We are already seeing advances in Artificial Intelligence (AI) with the EMRAD consortium which the Trust is part of. AI is currently being trailed by hospitals in Lincolnshire and Nottinghamshire to identify breast cancer in patients. It is hoped the project will combat staff shortages as the increase in imaging increases and improve the quality and efficiency in the service.

Cloud computing is another trend we can predict we will be using more often in healthcare, it has the potential to improve telemedicine, has better storage capacity at a lower cost. There are however disadvantages of cloud computing that must be taken into consideration, these include another organisation will be looking after the information and there will be limited control, along with the increased potential of insider threats and security.

APPENDIX C

Example of SARs requests going over the legislative timescale.

RFI	Number of Days	Explanation for breach of 30 day time limit
21129	31	Waiting for patient to decide how they wanted to receive the notes
22373	34 – request still open	Waiting for Dr to complete.
21942	32	Waiting for Dr to complete
21555	31	Notes in use
21292	34	Notes in use
20492	86	Extremely large sets of volume notes. Solicitors were aware and negotiated extended timeframe