Trust Board

Subject:	Senior Information Risk Owner (SIRO) Report for Trust Board	Date: 6th July 2023	
Prepared By:	Sally Brook Shanahan, Director of Corporate Affairs		
Approved By:	Sally Brook Shanahan, Director of Corporate Affairs		
Presented By:	Jacqueline Widdowson, Information Governance Manager & Data Protection Officer.		

Purpose			
The purpose of this report is to provide the Trust Board with an overview of the Trusts statutory and legal compliance with the Information Governance and Information Security Agenda and provide the final submission outcome of the DSPT.		**Approval**	
		Assurance	**x**
		Update	
		Consider	

Strategic Objectives

Provide outstanding care in the best place at the right time	Improve health and well-being within our communities	Empower and support our people to be the best they can be	To continuously learn and improve	Sustainable use of resources and estate	Work collaboratively with partners in the community
			x		

Principal Risk

PR1	Significant deterioration in standards of safety and care	**x**
PR2	Demand that overwhelms capacity	
PR3	Critical shortage of workforce capacity and capability	
PR4	Failure to achieve the Trust's financial strategy	
PR5	Inability to initiate and implement evidence-based Improvement and innovation	
PR6	Working more closely with local health and care partners does not fully deliver the required benefits	
PR7	Major disruptive incident	
PR8	Failure to deliver sustainable reductions in the Trust's impact on climate change	

Committees/groups where this item has been presented before

Elements of the report have previously been presented to the Audit Committee and Executive Team Meeting

Acronyms

DSPT – Data Security Protection Toolkit
IG – Information Governance
SIRO – Senior Information Risk Owner
IAO – Information Asset Owner
FOI – Freedom of Information
DPA – Data Protection Act
DPO – Data Protection Officer
ICO – Information Commissioner's Office

Executive Summary

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

The Annual SIRO report is included within Appendix A and provides an overview on our legislative and regulatory compliance with the FOI Act, DPA, DSPT and any incidents reported to the ICO.

All 113 of the 113 Mandatory standard evidence items are now complete for the DSPT. The DSPT has now been submitted with an overall compliance as standards met.

During 2022/23, 6 incidents were escalated as reportable to the Information Commissioners Office. None have resulted in action from the regulators as the Trust provided appropriate assurance.

Appendix B touches on the Data Saves Lives Strategy and how by harnessing the power of data, we will see the emergence of AI technology into the Trust.

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

2022/23 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 Security & Protection Toolkit and provide assurance of progress in relation to the requirements which are mandated for completion.

To inform the Trust Board about 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 2022/23 and how it aligned 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 the management of confidential information. The Committee monitors the completion of the Data Security & Protection Toolkit submission, data flow mapping, and information asset registers. The Committee also ensures the Trust has effective policies, processes, and management arrangements in place.

No outstanding standards remain for completion and the final submission has been made with all 113 standards met.

Data Flow Mapping & Information Asset Registers

To be legally compliant with data protection legislation, our organisation must keep a register of all the different types of information it stores, shares, and receives. The register also needs to detail all the digital and physical places where personal and sensitive information is stored, and how it is kept safe.

The SIRO is responsible for the development and implementation of the organisation's Information Risk agenda. During 2022/23 the IG Team circulated the Information Asset Register (IAR) and Data Flow Maps (DFM) for each business areas to ensure that all new systems and data flows were recorded, and risk assessed. We aim to disseminate and receive returns each year to ensure we have the most up to date registers in place. Some challenges were encountered in-year for reviews due to operational pressures across the services, staffing changes and staff shortages within the IG Team. The 3 main areas we are awaiting returns from are Medicine, Surgery and Women & Children's who had an extended deadline to the 30th June 2023.

The registers contain information such as:

- Key owners
- Retention periods
- Location of the data
- Media type (paper/ digital)
- Frequency of back up
- Access controls
- The legal basis for sharing
- Who the recipient of the data is

- Data transfers outside the UK

The IAR's & DFM's received were reviewed on 1ˢᵗ June 2023 by the IG Manager/ DPO and any gaps in information fed back to the relevant business areas, with support from the IG Team to complete.

At present the IAR & DFM for each business area are kept separately so they can be periodically updated as necessary throughout the year and return when requested. Moving forward this information will be transferred to the Corestream software environment to ensure that all the information is stored in one place and alerts will be generated automatically when a review is needed, thereby streamlining the process. A working group is currently being created to refresh the work of the IAO's and provide support in understanding the requirements of the role.

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 these are then reported through to the ICO.

To date there have been six incidents that have been reported on the Data Security & Protection Toolkit during 2022/23 of which only one required further investigation by the ICO. This has now been resolved with no further action taken.

Risk Management and Assurance

The SIRO is responsible for the development and implementation of the organisation's Information Risk agenda. During 2022/23 the IG Manager/ DPO has reviewed the current top 3 data risks with the Risk Manager, these have been identified as unsupported systems, training, and cyber security. A report was presented to the IG committee in June, along with an action plan in place for mitigation and to strengthen these areas.

Freedom of Information (FOI)

During 2022/23 to date the Trust processed a total of 710 FOIA requests. This function is managed by the IG Team and the activity is demonstrated in the table below. There has been a significant increase in the number of FOI requests received at the Trust than in the previous year. The Trust received 602 which is an increase of more than 100 requests. The IG Team continue to monitor the number of requests and going forward the IG Committee will monitor compliance. An FOI working group has been formed and it is hoped that this will support the teams across the Trust who provide information for the requests to attain compliance.

Total	Breached timeframe of 20 days	Escalated to ICO
710	248	0

This year has been challenging due to ongoing operational pressures which has had a continued impact on the number of FOI requests going over the 20 working days statutory timeframe.

Subject Access Requests

The Trust has received 3172 requests for access to patient records and 17 requests for employee records. The majority of patient records are processed in line with national guidance which is exemplary given that some of these cases represent hundreds of pages of information and require methodical attention to detail to ensure that 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. There has been a substantial increase of around 400 more requests received into the department during 22/23 than in previous year.

Type	1st April 2022 to 31st March 2023	Completed < 21 days	Completed 21-30 days	Completed > 30 days
Patient, Sols, Police	3172	2749	422	1
Employee	17	10	4	3

APPENDIX B

Horizon Scanning 2022/23

The data save lives: reshaping health and social care with data strategy, aims to commit to giving health and care staff the information they need to provide the best possible care and the NHS has an ambition to deploy more AI into the health and care environment.

It is hoped that the deployment of AI will support the prevention, early diagnosis, and treatment of chronic diseases. It will help clinicians diagnose conditions such as cancer, heart disease and stroke more quickly and in turn patients receive the treatment they need sooner.

There are models that can support not only the diagnosis and treatment of patients but also work processes. For example, process mining which can use a set of mathematic algorithms for extracting process flows from data generated by the process. This then can be used to analyse the data and processes for the accident and emergency department data flows.