Healthier Communities,
Outstanding Care

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

Board of Directors - Public

Subject:	Senior Information Risk Owner (SIRO) Report for Trust Board	**Date:** 1st April 2021
Prepared By:	Jacquie Widdowson, Information Governance Manager & Data Protection Officer	
Approved By:	Shirley Higginbotham, Director of Corporate Affairs , Paul Robinson, Chief Financial Officer & SIRO	
Presented By:	Paul Robinson, Chief Financial Officer & SIRO	

Purpose		
To provide assurance to Board of Directors on the compliance with the Data Security Protect Toolkit	**Approval**	X
	Assurance	
	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	

Overall Level of Assurance				
	Significant	**Sufficient**	**Limited**	**None**
Indicate the overall level of assurance provided by the report -		X		
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

None

Executive Summary

This report provides the Trust Board with an overview of the Trust’s compliance with the Information Governance (IG) and security agenda both nationally and locally.
The report has been updated in areas where appropriate real time information is available

The 2020/21 Annual SIRO report is included at Appendix A.
At present 108 of the 111 Mandatory evidence items are now complete, with plans to complete the remaining outstanding items by 31st March 2021. The outstanding areas are listed with current progress.

2 incidents have been escalated as reportable to the Information Commissioners Office during 2020/21. 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

2020/21 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 2020/21 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. Also ensuring the Trust has effective policies, processes and management arrangements in place.

Final preparations for final submission are being completed which is due 30th June 2021. At present 93 of the 111 Mandatory evidence items are now complete, with plans to complete the remaining outstanding items by 31st March 2021.

Assessment of completion & trajectory – including high risk areas.

As of 24th March 2021 the areas listed as outstanding are detailed below with an update on progress Evidence is updated on a daily basis and therefore this reflects the current point in time.

Standard 8

8.2.2 The SIRO confirms that risks of unsupported systems are being managed – paper presented at February IG Committee, more context to be added and recirculated.

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 – SOP being rewritten and will be presented at the next IG Committee.

Standard 9

9.4.6 What level of assurance did the independent audit of your Data Security Protection Toolkit provide to your organisation - awaiting outcome cannot be completed until report obtained.

Data Flow Mapping

The SIRO is responsible for the development and implementation of the organization's Information Risk agenda. During 2020/21 the Trust has undertaken an annual review of information flow mapping to ensure that we are assured that information flows into and out of the Trust are identified, risk assessed and addressed. This is then expanded to ensure that we have assurance that 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 number of returns received has been greater than in previous years and the data is much richer. One area identified for improvement is the response to having Business Continuity Plans (BCP) in place; some returns have not completed the column that one exists. The Information Asset Owner Framework that is currently being hopes to address this gap and provide assurance to the SIRO.

Information flows have been received 2020/21 from the following departments:
Anesthetics
Audiology
Cancer Services
Cardiology
Chaplaincy
Day Case
Dermatology
Estates & Facilities
Finance
HR
Information Services
Integrated Sexual Health Services
Management Secretaries
Medway
MEMD
NHIS
Pain Management
Pathology
Pharmacy
Pre-op
Programme Management Office
Risk & Assurance
Research & Development
Radiology
Respiratory
Rheumatology
Stroke
Training & Development
Trust Headquarters
Urgent & Emergency Care
Waiting List
Women & Children

Outstanding Data Flow Maps
Communications
Diabetes
Infection Prevention and Control Department
Patient Services
Therapy
All outstanding data flow maps will be chased and support given to complete by 31st March 2021.

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

- Add to the IG Checklist to review the pseudoymisation techniques or justification what type of data is to be used for the system/ project being implemented.
- Complete account access management SOP before implementation of a project, and add this to checklist.
- The new DPIA template captures the recording of the type of encryption used and what standard. When a new system is being implemented use the Trust template and transfer the data over from a supplier's template and add to the checklist
- To add physical security controls to the new Trust DPIA

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 2 incidents that have been reported during 2020/21 and 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 2020/21 the IG Manager/ DPO has reviewed the current top data risks which are unsupported systems, human error and availability of information, ongoing work will see the risks aligned to the current risk register. Gaps in the process of risk assessments and monitoring have been identified as part of the initial report on unsupported systems, the report will be developed further with mitigations and actions incorporated.

Freedom of Information (FOI)

During 2020/21 to date the Trust processed a total of 464 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	Escalated to ICO
464	115	1

This year has been challenging due to the current ongoing situation which has had an impact on the number of FOI requests going over the 20 day timeframe.

Of the 464 requests, 419 are currently completed, 8 on hold waiting further information and 37 still in progress. Of the 475 requests completed 274 have been completed within 20 days which show a compliance rate of 59%. The IG Team has addressed some processes areas where bottlenecks were occurring.

Subject Access Requests

The Trust has received 2471 requests for access to patient records. The majority of cases 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 decrease of around 500 requests received into the department during 2020/21 which we believe is due to the Covid-19 pandemic. Those requests that have been completed over 30 days are as a result of the Covid-19 pandemic, which impacted on staffing levels and requesting information from other departments.

1 March 2020 to 28 Feb 21 Total	Completed < 21 days	Completed 21-30 days	Completed > 30 days
2471	KM -1857 NWK -354 IG-11	KM- 222 NWK – 10 IG- 7	KM – 7 NWK - 0 IG - 3

APPENDIX B

Horizon Scanning 2020/21

The Cyber landscape is changing at a considerable rate and it is difficult to keep up to date with new and emerging technologies. The lines between information governance and data/ IT governance continue to overlap and as 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.

As we move into the future we will see the use of single sign on which will enable clinicians to move away from remembering multiple passwords and usernames. This will save both time and productivity and remove the need to encourage workarounds in busy departments such as accident and emergency, were sharing smartcards and generic accounts has caused IG incidents. We are also starting to see the use of biometrics which will allow clinicians to simply touch a finger print scanner to get instant access to systems

We have already seen a rapid growth in telemedicine in 2020 due to the pandemic and this is set to expand in 2021, with this more NHS staff are working from home which means that policies need to be robust and fit the user being onsite and working from home.

Another trend that is fast emerging due to Covid-19 is artificial intelligence, which is now looking at pandemic detection, vaccine development, thermal screening, facial recognition and analysing CT scans.

Mobile apps and devices are now playing a critical role in tracking the public to prevent illness, so we are now seeing the internet of medical things. As we use more technology we share more data electronically and therefore we increase the risk landscape and the increased risk of data loss as the threat landscape increases.