BOARD OF DIRECTORS (OPEN)
Meeting date: 13 November 2019

Open BoD 13.11.19
Item 11

TITLE OF PAPER	Senior Information Risk Owner (SIRO) Annual Report 2018/19
TO BE PRESENTED BY	Mr. P. Easthope, Interim Deputy Chief Executive/ Executive Director of Finance, IMST, Facilities & Performance
ACTION REQUIRED	For information and assurance

OUTCOME	To report progress and provide an overview and status of key areas covering during 2018/19, whilst identifying areas for improvement and strengthening for 2019/20.
TIMETABLE FOR DECISION	None required.
LINKS TO OTHER KEY REPORTS/DECISIONS	• NHS Digital & England Guidance • Data Security & Protection Toolkit • Cyber-Security Best Practices • Information Technology Service Management • General Data Protection Regulation • Caldicott Principles • Data & Information Quality Management • ISO27001 Information Security Management Systems
STRATEGIC AIM STRATEGIC OBJECTIVE BAF RISK NUMBER & DESCRIPTION	Strategic Aim: Value for Money Strategic Objective: A401 We will improve the productivity and efficiency of our services, maximising time spent with service users. BAF Risk Number: A401ii BAF Risk Description: Trust governance systems are not sufficiently embedded.
LINKS TO NHS CONSTITUTION & OTHER RELEVANT FRAMEWORKS, RISK, OUTCOMES ETC	As above.
IMPLICATIONS FOR SERVICE DELIVERY AND FINANCIAL IMPACT	-

CONSIDERATION OF LEGAL ISSUES	None required.
Author of Report	John Wolstenholme
Designation	Information Manager/Data Protection Officer
Date of Report	October 2019

SIRO Annual Report 2018/19

Item Ref: 11

Subject: **SIRO Annual Report 2018/19**

Presented by: **Phillip Easthope, Executive Director of Finance, IMST, Facilities & Performance**

Author: **John Wolstenholme, Information Manager/Data Protection Officer**

---

1. Purpose

For Approval	*For a collective decision*	*To report progress*	*To seek input from*	*For information*	*Other (please state below)*
		X			

2. Summary

2018/19 Senior Information Risk Owner (SIRO) annual summary position on the Trust's performance over the last 12 months on data and information governance challenges, risks, progress and focused commitment towards continuous data, information and system security and protection in accordance to:

- NHS Digital & England Guidance
- Data Security & Protection Toolkit
- Cyber-Security Best Practices
- Information Technology Service Management
- General Data Protection Regulation
- Caldicott Principles
- Data & Information Quality Management
- ISO27001 Information Security Management Systems

The report provides an overview & status for key areas covered during 2018/19, whilst identifying areas for improvement and strengthening for 2019/20.

Table of Contents

List of Tables and Figures

1 Role of the SIRO

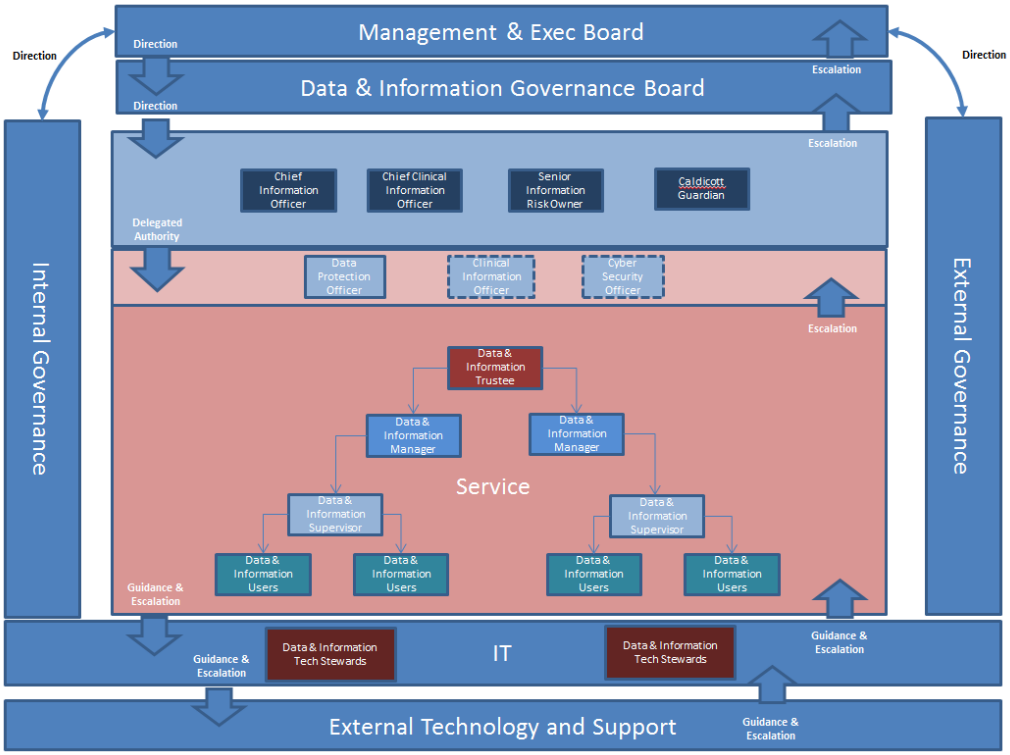
The Senior Information Risk Owner (SIRO) is responsible for the management of information risks within the organisation and for holding Directors and other Data & Information Asset Owners (DIAOs) to account for the management of information assets and related risks and issues within their areas of responsibility. The SIRO ensures that Information Governance, information and cyber security are dealt with at the highest level of management.

Within SHSC the SIRO is the Executive Director of Finance. The SIRO is a member of the Data & Information Governance Board (DIGB) and the Executive Directors Group (EDG).

The framework for the management of data and information within the Trust is set out in the Data and Information Governance Policy – this specifies the relationship between the SIRO, other senior information governance roles (including the Caldicott Guardian, the Chief Information Officer and the Chief Clinical Information Officer) and Data & Information Asset Owners. The network of DIAOs and reporting processes to the SIRO has gained traction in 2018/19 combining resources and key stakeholders from IMST, Quality and Clinical Operations departments.

Progress has been made through joint ownership of data, IT systems and governance which have resulted in increased assurance with the existing Data and Information Governance Structure seen below in Figure 1.

Figure 1- Data and Information Governance



2 2018/19 SIRO Summary Position

Table 1 below shows the SIRO Summary Position for 2018/19.

Area	Risk	Response	RAG
Policies	Policies maintained, reviewed and updated within agreed timescale.	All Data & Information polices reviewed and in date. Future review staggered to reduce further risk.	G
GDPR/DP	Maintain compliance, security and protection levels to GDPR requirement.	Further strengthening and transition required across the Trust. Plan in place to support positive progress in this area.	A
Incidents	Report and manage IG incidents to Trust policy and regulatory guidelines.	Systems & processes in place to deal with incidents and protect against threats. Tested and satisfied.	G
IG Toolkit	Maintain and provide evidence needed for DSPT compliance.	Work undertaken on the new DSPT requirements with supporting action plan. A review of 18/19 action and priority areas for 19/20 is scheduled for October 19.	A
Data & Information Assets	Identification and management of all Trust data & Information assets to ensure appropriate protections, controls and ownership in place.	Foundation register for data, information, systems and flows in place. Implementation of a new IT Service Management tool will provide further assurance and functionality in this area. The trust Performance Quality Framework will support further data asset assurance.	A
New Processing	New processing assessed, protected and controlled to Trust policy and regulatory requirements	IG considerations incorporated at the design stage. Evidenced with recent examples using Data Protection Impact Assessments and supported discussion through DPO, services and relevant boards.	G
Training & Awareness	Trust maintains training and awareness to support Trust wide compliance and understanding.	Required compliance level is 95% and requires focused attention to ensure target trajectory.	A
Risk Analysis	Ensure incidents & risks are reported, escalated and	Appropriate policies and processes in place to ensure	G

	managed according policy and response guidelines.	incidents are logged via and managed through corporate incident and risk register.	
IG Audits	Maintain audit action and compliance within agreed timescales.	Rating relates to the audit process and does not attempt to anticipate the findings of the audits	G
CQC	Manage, maintain and implement quality IG services to Trust and CQC expectations and targets.	No issues raised at this time.	G
SIRO Group	Maintain regional SIRO engagement and discussion	Local SIRO group has been disbanded. Contacts maintained via other IG forums,	G
Priorities	Maintain and implement agreed, statutory and mandatory IG commitments and continuous improvement programmes.	Raised as amber due to resource capacity and associated work required to deliver and additional responsibilities required for GDPR, DSPT & DPO. Risk should to be reduced through automation, increased trust wide responsibility and transfer of some tasks to other IG staff.	A

Table 1 - SIRO Summary Position

3 2018/19 Position Update

3.1 IG Policies

Area	Risk	Response	RAG
Policies	Policies maintained, reviewed and updated within agreed timescale.	All Data & Information polices reviewed and in date. Future review staggered to reduce further risk.	G

Figure 2 below shows the suite of Information Governance policies have been revised and updated. There is an outstanding action to review the Data, Information and System Asset Management Policy (due 31/03/2019) and a Recording Policy is in development.

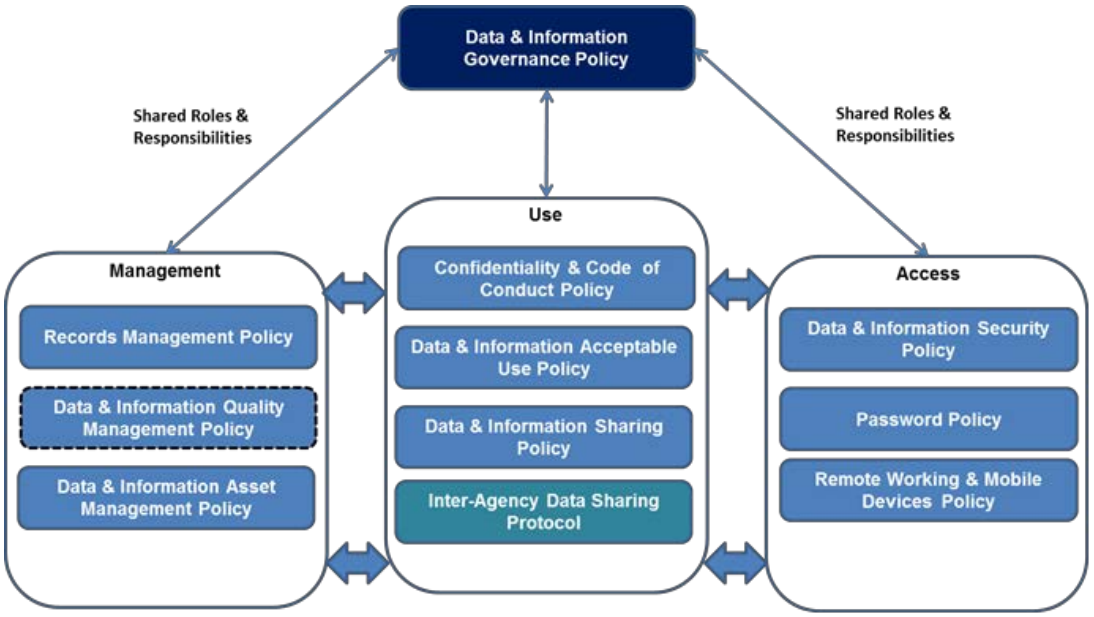


Figure 2 - Updated Information Governance Policies

3.2 GDPR/Data Protection Act 2018

Area	Risk	Response	RAG
GDPR/DP	Maintain compliance, security and protection levels to GDPR requirement.	Further strengthening and transition required across the Trust. Plan in place to support positive progress in this area.	A

Transition work to comply with the General Data Protection Regulation/Data Protection Act 2018 complete. Further supporting process work to embed knowledge transfer and trust wide awareness requirement to ensure new GDPR requirements are embedded into trust processes, projects and service commissioning. Greater reporting of incidents and risk management through trust risk and issue reporting system.

3.3 IG Incidents

Area	Risk	Response	RAG
Incidents	Report and manage IG incidents to Trust policy and regulatory guidelines.	Systems & processes in place to deal with incidents and protect against threats. Tested and satisfied.	G

Information Governance incidents and risks are reported internally with other incidents via the Trust incident monitoring system. Increased trend in incident reporting statistics with lessons learned shared to support further knowledge transfer. Those with an IG element are graded in terms of seriousness and any which reach a specified level are reported externally to the ICO.

The Data Security & Protection Toolkit (DSPT) incident reporting tool has been used successfully to report serious incidents and near misses.

During 2018/19 the Trust submitted one incident via the DSPT reporting tool which qualified for onward notification to the ICO. This concerned patient information sent to the Parliamentary & Health Service Ombudsman which was reported to be excessive.

Information governance incidents are reported to the DIGB as a standing agenda item.

Notification of Cyber security risks from CareCERT are received and acted upon by the IT Department. IMST service improvement work in progress for computer hardware, software and security patch management.

3.4 Data Security & Protection Toolkit (DSPT)

Area	Risk	Response	RAG
IG Toolkit	Maintain and provide evidence needed for DSPT compliance.	Work undertaken on the new DSPT requirements with supporting action plan. A review of 18/19 action and priority areas for 19/20 is scheduled for October 19.	A

The first Data Security and Protection Toolkit submission was submitted in October 2018 and a final submission in March 2019. Progress of DSPTK is monitoring through DIGB

At time of submission the Trust's assessment was that it did not meet all mandatory requirements within the DSPTK so an improvement plan to meet the required standard was agreed with NHS Digital with a target completion date of September 2019.

3.5 Data & Information Assets and Flows

Area	Risk	Response	RAG
Data & Information Assets	Identification and management of all Trust data & Information assets to ensure appropriate protections, controls and ownership in place.	Foundation register for data, information, systems and flows in place. Implementation of a new IT Service Management tool will provide further assurance and functionality in this area. The trust Performance Quality Framework will support further data asset assurance.	A

GDPR and the Data Security & Protection Toolkit require the Trust to maintain a register of information assets and flows of personal data. Progress has been made to maintain an electronic asset register of IT Systems and key information asset stakeholders. This is further improved through the implementation of a new IT Service Desk tool. Improvements to data ownership, reporting and assurance is led trough the trust Performance Quality Framework which continues to gain momentum.

3.6 New Processing

Area	Risk	Response	RAG
New Processing	New processing assessed, protected and controlled to Trust policy and regulatory requirements	IG considerations incorporated at the design stage. Evidenced with recent examples using Data Protection Impact Assessments and supported discussion through DPO, services and relevant boards.	G

Data Protection Impact Assessments are undertaken for all new data and IT system requests to support the identification of potential risks and how they may be mitigated.

Online cloud storage requests are managed stringently, the development of cloud storage use policies are in progress to ensure the necessary safeguards are in place to support cloud storage use.

Major projects and processes are governed by the Digital Transformation Strategy.

3.7 Training and Awareness

Area	Risk	Response	RAG
Training & Awareness	Trust maintains training and awareness to support Trust wide compliance and understanding.	Required compliance level is 95%. Regular progress reporting led by Mandatory Training Steering Group and regular gap analysis.	A

The SIRO has completed specific, relevant training in support of his role.

All staff are required to complete the mandatory national information governance training on an annual basis. Compliance is monitored and reported by the Mandatory Training Steering Group. Staff awareness undertaken highlighting key points on GDPR and DSPT delivered in 2018/19.

The Data & Information Governance & GDPR SharePoint page is updated on a regular basis.

3.8 Risk Analysis

Area	Risk	Response	RAG
Risk Analysis	Ensure incidents & risks are reported, escalated and managed according policy and response guidelines.	Appropriate policies and processes in place to ensure incidents are logged via and managed through corporate incident and risk register.	G

Information Governance risks including cyber security risk are reported to the DIGB. Sufficiently serious risks are included in the Corporate Risk Register.

Regular updates on DIAOs reported through DIGB and SIRO. All digital project requests go through a robust process to identify and mitigate risks during project initiation. Greater risk analysis and reporting through SHSC trust risk management system, external reporting systems and project and portfolio reporting procedures.

3.9 IG Audits

Area	Risk	Response	RAG
IG Audits	Maintain audit action and compliance within agreed timescales.	Rating relates to the audit process and does not attempt to anticipate the findings of the audits	G

The SIRO oversees the audit programme for the Trust. During 2018/19 the following IG-related audit reports were received:

Data Security & Protection Toolkit – Limited Assurance
Early Intervention in Psychosis (Data Quality) – Significant Assurance
Clinical Coding – Level 3 (maximum)

3.10 CQC Inspection

Area	Risk	Response	RAG
CQC	Manage, maintain and implemented quality IG services to Trust and CQC expectations and targets.	No issues raised at this time.	G

The SIRO and CIO were key contacts for the CQC inspection of the Trust in July 2018. No significant IG-related issued were identified.

3.11 South Yorkshire SIRO Group

Area	Risk	Response	RAG
SIRO Group	Maintain regional SIRO engagement and discussion	Local SIRO meeting disbanded	G

The previous local SIRO group has been disbanded but SIRO issues are covered by other Information Governance forums including the Directors of Information and SIGN groups. Bilateral contacts with partner organisations are made if necessary.

3.12 Priorities for 2019/2020

Area	Context	Response	RAG
Priorities	Maintain and implement agreed, statutory and mandatory IG commitments and continuous improvement programmes.	Remains as amber due to resource capacity and associated work required to deliver and additional responsibilities required for GDPR, DSPT & DPO. Risk will be reduced through with embedding trust wide responsibility, automation and supporting tools.	A

Priorities for 2019/20 are listed below:

- Strengthening GDPR and DSPT requirements through improved supporting tools including a new IMST service desk, automatic reporting procedures and wider communication of key messages.
- Continue to develop the DSPT work programme.
- Data and Cyber Security incident planning and testing. Actions from recent planned penetration test have shown the trust has good network security and system controls in place and a proactive approach to security but requires some further development in security patch management.
- Audit action.
- Data Protection duties and support.

4 Actions

The SIRO report will be developed into a more comprehensive report for 2020/21 to which will contain a summary of information requests, incidents and lessons learned, detailed analysis of DSPT, Mandatory Training statistics and areas of concern and information risks.

This report is presented for assurance to the Finance, Information & Performance Committee, having been received and considered by the Digital Information Governance Board (DIGB).

5 Monitoring Arrangements

Monitoring progress on a regular basis via DIGB.

6 Contact Details

John Wolstenholme, Data Protection Officer