Board of Directors - Public

14 July 2022

Paper title:	Annual Report / Senior Information Risk Owner (SIRO)	**Agenda item**
Presented by:	Tim Rycroft, CIO	
Prepared by:	Gaynor Toczek, Data protection Officer	**23**

Purpose of the report		
This annual report provides the Trust Board with an update relating to the responsibilities of the SIRO and outlines activity and performance related to information governance. It provides assurances that information risks are being effectively managed, what has been achieved and where improvements are required going forward.	For approval	
	For discussion	
	For information	X

Executive summary

This annual report documents:

- Compliance with legislative and regulatory requirements relating to the handling of information, including compliance with the Data Protection Act (2018) and the Freedom of Information Act (2000)
- Informs the Board of information security risk assessments
- Details compliance with the Data Security and Protection Toolkit 2021/2022
- Provides assurance of ongoing improvements in relation to managing information risks
- Details any Serious Incidents relating to personal data or breaches of confidentiality
- Outlines the direction of information governance work for 2022/2023

Do the recommendations in this paper have any impact upon the requirements of the protected groups identified by the Equality Act?	**State below 'Yes' or 'No'**	If yes please set out what action has been taken to address this in your paper
	No	

Recommendation

The Board of Directors is asked to:

- Consider the information and assurances provided for 2021/2022
- Note the proposed information governance objectives for 2022/2023

Strategic vision Please mark those that apply with an **X**				
Providing excellent quality services and seamless access	**Creating the best place to work**	**Supporting people to live to their fullest potential**	**Financial sustainability growth and innovation**	**Governance and well-led**
				X

Care Quality Commission domains Please mark those that apply with an **X**				
Safe	**Effective**	**Responsive**	**Caring**	**Well Led**
X		**X**		**X**

Relationship to the Board Assurance Framework (BAF)	The work contained with this report links to the following strategic risk(s) as identified in the BAF: •
Links to the Strategic Organisational Risk Register (SORR)	The work contained with this report links to the following corporate risk(s) as identified in the SORR: • 2046
Compliance and regulatory implications	The following compliance and regulatory implications have been identified as a result of the work outlined in this report: • Data Protection Act 2018 • Freedom of Information Act 2000 • UK General Data Protection Regulation 2018 • Data Security and Protection Toolkit

Meeting of the Board of Directors - Public

14 July 2022

Annual Report - Senior Information Risk Owner (SIRO)

---

1. Background and Context

The Trust recognises the value of the data within its information systems. The Trust also recognises its responsibility to ensure the appropriate use, security, reliability, and integrity of this data; to safeguard it from accidental or unauthorised access, modification, disclosure, use, removal, or destruction; and to comply with relevant legislation.

The Trust is a recognised and registered Data Controller within the Information Commissioner's Data Protection Register and has current Data Protection registration. There are no current or historical conditions or cautions against the Trust's data protection registration.

1.1 Key responsibilities of the Senior Information Risk Owner

The key responsibilities of the SIRO include:

- Overseeing the development of the Information Governance policy.
- Ownership of the assessment processes for information risk, including prioritisation of risk and review of the annual information risk assessment to support and inform the Annual Governance Statement.
- Ensuring the Trust Board is fully informed of key information risks.
- Reviewing and agreeing actions in respect of identified information risks.
- Ensuring the effective implementation of the Information Asset Owner / Information Asset Administrators (IAO / IAA) infrastructure to support the role of the SIRO.
- Ensuring that identified information threats and vulnerabilities are investigated for risk mitigation, and that all perceived or actual information incidents are managed in accordance with BDCFT's Incident Management policy; and
- Ensuring effective mechanisms are established for the reporting and management of Serious Untoward Incidents relating to the information of the Trust, maximising the opportunity to ensure learning from incident reporting.

1.2 Information Governance Group (IGG)

The IGG meets bi-monthly and is responsible for ensuring the effective management of the Trust's information governance processes, reporting to the Digital Strategy Group quarterly about how risks are being managed.

Chaired by the SIRO, the key duties of the IGG include:

- Review and monitoring of the Trust's compliance with the Data Security and Protection Toolkit (DSPT).
- Review and monitoring of the Trust's annual Information Governance Strategy and Plan.
- Review and monitoring of any information governance risks, ensuring appropriate escalation to the Board.
- Review and monitoring of new and changing information assets in compliance with the requirements of the DSPT.
- Reviewing all information governance policies and procedures.
- Monitoring trends from incident reporting.
- Ensuring the Trust has an information governance training programme.

The Trust's Information Governance Assurance Framework is underpinned by Trust policies, available on Connect including:

1. Acceptable Use policy.
2. Confidentiality and Data Protection policy.
3. Records Management policy.
4. Bring Your Own Device (BYOD) policy.
5. Freedom of Information policy.
6. Clinical Systems Data Quality policy
7. Information Governance policy.
8. Information Technology Acceptable Use policy.
9. CCTV policy.
10. Information Security policy.
11. Social Media policy.
12. Printing policy.
13. Clinical Systems Security policy.
14. DPIA procedure.
15. Removable Media policy.
16. Risk Management policy.
17. Incident Management policy.
18. Employment policy includes the Mandatory and Required Training policy and the Registration Authority (RA) policy.

1.3 Data Security and Protection Toolkit (DSPT)

The DSPT is an online tool that enables organisations to measure and publish their performance against the National Data Guardian's ten security standards:

1) **Personal Confidential Data**: All staff ensure that personal confidential data is handled, stored, and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

2) **Staff Responsibilities:** All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

3) **Training:** All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit.

4) **Managing Data Access:** Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

5) **Process Reviews:** Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

6) **Responding to Incidents:** Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

7) **Continuity Planning:** A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management

8) **Unsupported Systems:** No unsupported operating systems, software or internet browsers are used within the IT estate.

9) **IT Protection:** A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually

10) **Accountable Suppliers:** IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards

2. Status of Organisational Compliance

2.1 Data Security and Protection Toolkit (DSPT) 2021/2022

To be compliant with the toolkit in 2021/2022 all evidence marked as "mandatory" needs to have been met. There are 110 mandatory evidence items in total underpinning 142 assertions.

The final version of the DSPT will be submitted at the end of June 2022.

2.3 Internal audit

During 2021/22 Audit Yorkshire conducted an audit of the Trust's DSPT. The draft DSPT audit report has been given an overall confidence level of **Medium**, which is equivalent to **Significant Assurance.**

The auditor identified 3 significant findings and provided recommendations, which the Trust is working towards addressing ahead of the final submission.

.

The auditor found the following examples of good practice within the Trust:

- Data Security and Data Protection training provided to all new starters.
- Adoption of a comprehensive approach to Data Protection by Design and Default, with a Pseudonymisation policy in place. Data protection has been adopted into wider business, alongside significant technical controls to prevent information being inappropriately downloaded.
- A Cyber Incident Response Plan is in place along with local Business Continuity Plans. A tabletop exercise of the Cyber Incident Response Plan was undertaken in March 2022.
- An IT Health Check was undertaken by NHS Digital in November 2021, tests are performed and supported by action plans, to help ensure that risks from unauthorised access to the network are minimised.
- The audit review identified a comprehensive process for the management of alerts received, involving the containing and investigation of these.
- The Foundation Trust has a patch management process in place, which is supported by management reporting on key performance indictor data.

2.4 Serious Incidents Requiring Investigation (SIRI) in 2021/22

Information governance (IG) incidents are reported internally through the web-based incident reporting system (IR-e) and notified immediately to the Information Governance (IG) & Records Manager. It is a legal obligation to notify personal data breaches 72 hours, to the ICO, unless it is unlikely to result in a risk to the rights and freedoms of individuals.

Notification is completed by logging incidents on the Data Security and Protection Toolkit (DSPT). All incidents assessed as being Serious Incidents Requiring Investigation (SIRI) are logged with the Trust's Serious Incident Lead. Incident data is regularly reported to and monitored by the IGG.

There were two incidents reported to the Information Commissioner's Office (ICO) and Department of Health and Social Care (DHSC) in 2021/22.

One related to three letters containing very sensitive and detailed information about one patient sent to the wrong address. The ICO determined that no further action is necessary but has made some recommendations for the Trust to consider.

One related to the unauthorised access to a clinical record by a member of staff. The ICO determined that no further action is necessary but made some recommendations for the Trust to consider. They also acknowledged the action plan that is in place to help prevent further incidents.

Details are provided below in the required format:

Date of incident (month)	Nature of incident	Number affected	How patients were informed	Lesson learned
October 2021	3 letters containing very sensitive and detailed information sent to the wrong address	1	Duty of Candour letter sent by the Medical Director.	Improved communications to clinical staff to ensure they are aware of changes to administrative processes.
October 2021	A patient raised a complaint relating to unauthorised access to his clinical record by a member of staff.	1	ICO informed the Trust of the patient's complaint.	Improve and reiterate communications to all staff of the importance of data security. Emphasising to all staff their obligations under Trust policy and data protection regulation.

In response to the first incident admin services updated their Standard Operating Procedure to instruct staff on how to update the main address on SystmOne for Mental Health Services. This refined process has been circulated to clinical teams to share with staff.

In response to the second incident the Deputy Chief Executive/Director of Nursing, the Medical Director and CIO communicated with staff reiterating the standards around record keeping and reinforcing messages around records management and accessing clinical records. Communicating amongst staff the importance of data security and reiterating the significance of good data protection practice should be done frequently.

2.5 Incidents reported in 2021/2022

Summary of Other Personal Data Related Incidents in 2020/21

Breach Type	
Availability	
Corruption or inability to recover electronic data	2
Unauthorised or accidental loss	184
Denial of Service (Not Cyber)	33
Lost or stolen paperwork	13
Lost in Transit	4
Loss or stolen unencrypted device	0
Lost or Stolen Hardware	23
Loss or theft of only copy of encrypted data	0
Data left in insecure location	20
Cyber incident (other DDOS etc)	0
Cyber incident (exfiltration)	0
Cryptographic flaws (e.g. failure to use HTTPS; weak encryption)	0
Non-secure disposal – hardware	0
Malicious internal damage	0
Non-secure disposal – paperwork	1
Confidentiality	
Disclosed in Error	51
Phishing emails	1
Data sent by email to incorrect recipient	22
Uploaded to website/intranet in error	1
Unauthorised upload to social media	1
Data posted or faxed to incorrect recipient	17
Unauthorised access/disclosure	25

Spoof website	0
Failure to redact data	0
Cyber bullying	1
Verbal disclosure	5
Failure to use bcc when sending email	6
Cyber security misconfiguration (e.g., inadvertent publishing of data on website; default passwords)	0
Hacking	1
Cyber incident (key logging software)	0
Integrity	
Unauthorised or accidental alteration	4
Website defacement	0
Cyber incident unknown	0
Other	198
Total	613

3. Risk Management and Assurance

3.1 Information Assets

Keeping an up-to-date Information Asset Register and monitoring data flows supports the confidentiality, integrity and availability of all information and data the Trust holds in physical and electronic Information Assets.

The Information Asset Register is updated throughout the year, with a major update in Quarter 3. All assets are assigned to an Information Asset Owner (IAO). Following the annual major update in Quarter 3 all risks to assets and data flows from the same are assessed. This risk assessment helps IAOs to make improvements to the security of their assets in advance of the DSPT submission in March each year. The collection and risk assessment also serve to keep the SIRO informed. IAOs are asked to complete monitoring forms containing details of their assets together with any data flows from those assets.

To complete the collection all IAOs and Information Asset Assistants (IAAs) are provided with guidance and are required to complete refresher training each year. This process helps to provide assurance to the SIRO on the security, reliability, and integrity of all information assets together with an up-to date risk assessment. Information held in assets may relate to service users, staff, and others: customers, suppliers, contractors, agents, elected members, volunteers, charitable groups, partners, and other business contacts.

Examples of information assets include database and data files, back-up and archive data, audit data, paper records and reports, people, skills and experience, application, and system software etc. Through reporting to IGG, the Information Governance and Records Coordinator has identified 147 Information Assets operating across the Trust. Where risks are identified associated with an asset, these are placed on the relevant risk register and monitored by the IGG.

3.2 Information Asset Owners and Administrators

The responsibilities and accountabilities of IAOs are to:

- understand and address risks to the information asset they 'own'; and
- be accountable to the SIRO to provide assurance on security and use of these assets.

The responsibilities and accountabilities of IAAs are to:

- ensures policies and procedures are followed.
- recognise potential or actual security incidents.
- consult their IAO on incident management; and
- ensure that information asset registers are accurate and up to date.

As of November 2021, the Trust identified 42 IAOs and 71 IAAs.

3.3 Organisations and Contractors

The Information Governance and Records Manager together with the IAOs has identified 42 organisations or contractors with whom we share information. Work is scheduled to ensure the Trust has either a contract or an up-to-date information sharing agreement (ISA) with each organisation or contractor.

3.5 Information Governance Risks

During 2021/22 the Trust had 5 information governance risks (including cyber security) on its service level Risk Register, 1 of which was closed and archived in year.

All live risks are monitored and have actions against them.

3.6 Information security

Data security is actively managed by both the Information Governance and Cyber Security teams within informatics.

Information governance and data security risks are monitored by the Information Governance Group (IGG) and are included in the DPST assessment. The IGG reports quarterly to the Digital Strategy Group (DSG). The DSG oversees the strategic aspects of the Trust's IT and digital technology agenda. The Cyber Security Manager reports weekly to the Chief Information Officer (CIO)/SIRO identifying events, actions and any security enhancements made to progress the security targets set by the Trust.

Weekly CareCERT bulletins are reviewed, risks identified and escalated appropriately, with immediate remediation work scheduled.

The Cyber Security team has been very proactive in implementing new cyber defences. It has taken an innovative approach to data security with the creation of a new Cyber Security Awareness campaign. This campaign will ensure staff are aware of the cyber security risks around them and be more comfortable in reporting the same. The team has implemented a series of new systems and programmes of work to monitor the security of the IT environment and has been working to further enhance the Trust's data protection and infrastructure defence.

The Trust is a national leader in email security being the first to fully implement NHS Digital's new e-mail security standard which has been maintained continuously.

The Trust complies with the requirements of the Cyber Essentials Plus scheme and was certified on the 11th of September 2021.

The team has also engaged in partnership with other trusts and organisations in tackling system-wide attacks which enhances the security of our system and processes in taking reactive actions affecting regional/national systems.

3.7 Information Sharing

The Trust recognises it has a responsibility to work with partners to minimise the burden of data collection and ensure that data is used effectively to support the overall aims of public sector and voluntary organisations, ensuring the delivery of safe, quality, clinical care. The Trust is a signatory of the Interagency Information Sharing Protocol, which is to be reviewed in October 2022, in which the Trust actively contributes and has Information Sharing Agreements with many partners.

3.8 Freedom of Information Requests (FOI)

During 2021/22, the Trust received a total of 380 requests under the Freedom of Information Act. 278 requests were managed within the twenty working day timescale (73%).

3.9 Requests for Personal Information

During 2021/22 the Trust received 647 requests for personal information 303 of which were Subject Access Requests (SARS) and 344 were Third Party Requests (TPRs).

3.10 Subject Access Requests (SARs)

The Data Protection Act 2018 gives individuals the right to find out what personal data the organisation holds about them. Such requests are termed Subject Access Requests (SARs) and have a statutory response time of 1 calendar month from date of receipt. Correct and prompt management of SARs increase levels of trust and confidence in the organisation by being open with individuals about the personal information held about them. Of the SARs completed in this period 275 (96%) were responded to within the required timescale.

3.11 Third Party Requests (TPRs)

There is no statutory deadline for requests made by third parties (TPRs), however there is an expectation they will be processed within 40 working days. 99% of the 333 Third Party Requests completed in this period were responded to within 40 days.

3.12 Data Assurance Corporate Records Audit

The Trust recognises its responsibility to ensure the appropriate use, security, reliability, and integrity of data; to safeguard it from accidental or unauthorised access, modification, disclosure, use, removal, or destruction; and to comply with relevant legislation. The corporate records audit addresses these responsibilities.

In keeping with the principles of the Data Protection Act (2018) the Trust has an annual Data Assurance and Corporate Records Audit.

Identified Information Asset Owners (IAOs) are tasked annually to complete the required assurance template for each of the systems in BDCFT that contribute key information and data for business decision. This year IAOs were also asked to provide evidence to support their assessments. Six systems were scrutinised in 2021/22:

a) SystmOne (clinical)
b) Safeguard (Complaints, Litigation, and Incident Management)
c) ESR (Workforce)
d) Oracle (Finance)
e) Payroll/ESR
f) R4 (Clinical – Dental)

3 potential risks were identified.

4. Summary of Key Achievements in 2021/22

4.1 The following were achieved during 2021/22 in relation to Information Governance:

- Review and analysis of the DSPT.
- Full compliance with the mandatory requirements of the DSPT.
- Completion of the actions in the Information Governance strategy and plan.
- Only 2 serious incidents recorded on the DSPT.
- Review and ratification of several key information governance policies, including:
    - Information Governance policy
    - Records Management policy
    - Confidentiality and Data Protection policy
    - Freedom of Information policy
    - Information Security policy
    - Social media policy
    - Bring Your Own Device (BOYD) policy

- Creation of a new Printing policy
- Reviewed and revised the IG Staff handbook
- Further embedding of information governance awareness through the IG staff survey results.
- Annual review and update of the Information Asset Register and bulk data flows.
- Completion of the Data Assurance and Corporate Records Audit.
- High audit assurance for DSPT.
- Completion of the IGG workplan.
- Regular scrutiny of information governance performance through the IG dashboard.
- Introduction of additional IG security assurances.
- Gained cyber essentials plus certification.
- Strengthened governance processes with IAOs and IAAs.
- Thorough reorganisation of archived records processes.
- Reviewed and further embedded the Data Protection Impact Assessment (DPIA) process.
- Embedded the Data Protection Impact Assessment review group to ensure requests for changes to the collection and use of personal data.
- Thorough review of Information Sharing Agreements.
- Embedded the Clinical Systems Access review group and underlying process to ensure new requests for clinical systems access are streamline and documented.
- Completely renewed the IG&RM pages on Connect.
- Supported the Trust with its move towards the sharing out of clinical records where consent is received.

5. Plans for 2022/23

5.1 The following Information Governance objectives are to be considered for 2022/23:

- To meet all new and existing standards within the DSPT.
- Maintain cyber essentials plus certification
- To deliver a new training strategy for information governance and security management.
- To maintain a low level of information governance serious incidents requiring investigation.
- Implement a new system for recording requests for information.
- To rationalise and improve the privacy notices available to patients and service users.
- To introduce a revised Publication Scheme to help reduce management time spent on responding to routine Freedom of Information requests.
- To further embed the Privacy Impact Assessment process (Privacy by Design and Default).
- To understand and embed any new requirements of the UK General Data Protection Regulation (UKGDPR) and Data Protection Act 2018.
- To continue to raise the profile of data sharing across the Trust and Health and Social Care.
- To further engage IAOs/IAAs through regular meetings
- To improve compliance with IAO/IAA training levels.
- To review the Information Asset Register and Bulk Data flows collection to ensure compliance with legislation.
- To embed the new Data Security staff survey.
- To ensure the Trust is in full compliance with the Jay (Goddard) Inquiry.
- To ensure the Trust is in full compliance with the COVID inquiry.
- To review existing IG related policies and procedures on the Group's work programme.
- To monitor the information governance implications of changes to clinical information systems.
- To review cyber security incidents monthly
- To escalate any risks or areas of concern to the Digital Strategy Group via quarterly reports and in the case of any significant security incidents to report these directly to Trust Board.
- To comply with the National Data, Opt-Out.
- To further enhance the IG and Cyber Security dashboard.
- To progress the use of Microsoft teams as a joint resource for information sharing agreements and explore the same to capture data protection impact assessments across the place.
- To support the Trust to enhance integrated working across the PLACE and the Act as One process.
- To understand and embed any new requirements to support the Trust to comply with the NHSX IG Framework.

The next Annual Report to the SIRO will be produced in May 2023.

6. Recommendations:

That the Board:

- note the assurances provided in the paper; and
- note the proposed information governance objectives for 2022/2023.

7. Implications

7.1 Legal and Constitutional

The Trust acknowledges the importance of demonstrating good practice against information governance standards and compliance with the Data Security and Protection toolkit.

8. Quality and Compliance

The Trust acknowledges the importance of demonstrating good practice against information governance standards and compliance with the Data Security and Protection toolkit.

9. Risk Issues Identified

Risk	Likelihood High/Medium/Low	Implication	Mitigation
Non-compliance with information governance requirements operating as an FT.	**Medium**	**Reputational damage and potential financial consequences imposed by regulators.**	**Existing governance arrangements (Digital Strategy Group and Information Governance Group) and risk escalation processes.**

Name of author/s / Gaynor Toczek
Title/s / Data Protection Officer
Date paper written / 26/05/22