Bradford District Care
NHS Foundation Trust

# Board of Directors – Meeting held in Public.

## 13 July 2023

| | | |
|---|---|---|
| **Paper title:** | Senior Information Risk Owner Annual Report | **Agenda Item** **18** |
| **Presented by:** | Tim Rycroft / CIO & SiRO | |
| **Prepared by:** | Gaynor Toczek / Data Protection Officer (DPO) | |

| | |
|---|---|
| **Committees where content has been discussed previously** | |
| **Purpose of the paper**<br>Please check **ONE** box only: | ☐ For approval ☒ For information<br>☐ For discussion |
| **Link to Trust Strategic Vision**<br>Please check **ALL** that apply | ☐ Providing excellent quality services and seamless access<br>☐ Creating the best place to work<br>☐ Supporting people to live to their fullest potential<br>☐ Financial sustainability, growth and innovation<br>☒ Governance and well-led |
| **Care Quality Commission domains**<br>Please check **ALL** that apply | ☒ Safe ☐ Caring<br>☐ Effective ☒ Well-Led<br>☒ Responsive |

## Purpose of the report

The Senior Information Risk Owner (SIRO) annual report provides 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.

## 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 2022/2023
- provides assurance of ongoing improvements in the relation to managing risks to information
- details any Serious Incidents relating to personal data or breaches of confidentiality.
- outlines the direction of information governance work for 2023/2024

| | |
|---|---|
| Do the recommendations in this paper have any impact upon the requirements of the protected groups identified by the Equality Act? | ☐ **Yes** (please set out in your paper what action has been taken to address this)<br>☒ **No** |

| **Recommendation(s)** |
|---|
| The Board of Directors is asked to:<br>• consider the information and assurances provided for 2022/2023<br>• note the proposed information governance objectives for 2023/2024 |

| **Relationship to the Board Assurance Framework (BAF)** | |
|---|---|
| The work contained with this report links to the following strategic risks as identified in the BAF:<br>☐ **SO1**: Engaging with our patients, service users and wider community to ensure they are equal partners in care delivery (QSC)<br>☐ **SO2**: Prioritising our people, ensuring they have the tools, skills and right environment to be effective leaders with a culture that is open, compassionate, improvement-focused and inclusive culture (WEC)<br>☐ **SO3**: Maximising the potential of services to delivery outstanding care to our communities (QSC)<br>☒ **SO4**: Collaborating to drive innovation and transformation, enabling us to deliver against local and national ambitions (Board)<br>☐ **SO5**: To make effective use of our resources to ensure services are environmentally and financially sustainable and resilient (FBIC)<br>☒ **SO6**: To make progress in implementing our digital strategy to support our ambition to become a digital leader in the NHS (FBIC) | |
| **Links to the Strategic Organisational Risk register (SORR)** | The work contained with this report links to the following corporate risks as identified in the SORR:<br>•<br>• |
| **Compliance & regulatory implications** | The following compliance and regulatory implications have been identified as a result of the work outlined in this report:<br>• Data Protection Act 2018<br>• Freedom of Information Act 2000<br>• UK General Data Protection Regulation 2018<br>• Data Security and Protection Toolkit |

# Board of Directors – Meeting held in Public

# 13 July 2023

---

# 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.

*Information regarding the role of the SIRO the Information Governance Group and the 10 security standards the Data Security Protection Toolkit can be found in appendices 2.

## 2. Status of Organisational Compliance

### 2.1 Data Security and Protection Toolkit (DSPT) 2022/2023

To be compliant with the toolkit in 2022/2023 all evidence marked as "mandatory" needs to have been met. There are 113 mandatory evidence items in total underpinning 131 assertions. The final version of the DSPT was submitted on 29th June 2023.

### 2.2 Internal Audit Assurance

During 2022/23 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.

### 2.3 Serious Incidents Requiring Investigation (SIRI) in 2022/23

Information governance (IG) incidents are reported internally through the web-based incident reporting system (IR-e) and notified immediately to the Data Protection Officer, Data Protection Manager and the 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 no incidents reported to the Information Commissioner's Office (ICO) and Department of Health and Social Care (DHSC) in 2022/23.

## 3. Incidents reported in 2021/2022

**Summary of Other Personal Data Related Incidents in 2022/2023**

| Breach Type | Numbers |
|---|---|
| Availability | 526 |
| Confidentiality | 229 |
| Integrity | 13 |
| **Total** | **768** |

*A detailed breakdown of the breach types is presented in appendices 1

## 4. Risk Management and Assurance

### 4.1 Information Assets and Information Asset Register

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. All assets are assigned to an Information Asset Owner (IAO) as are risks to assets and bulk data flows. The risk assessments help IAOs to make improvements to the security of their assets in advance of the DSPT submission. The collection and risk assessment also serve to keep the SIRO informed. IAOs are asked to update details of their assets together with any data flows from those assets.

During 2022/23 a major review of the Information Asset Register and method of collection of data relating to the register and data flows from these assets has been undertaken. This was done in conjunction with a subgroup of the IGG. The register was previously an excel database that was updated on an annual basis by IAOs.

The new register is a more interactive system that allows IAOs and IAAs to update information relating to their asset and bulk data flows. IAOs can also register new assets and identify when assets are decommissioned. These updates and additions take place on a rolling basis with IAOs, and IAAs informed that a review is required if a review has not taken place in the previous 12 months. The new system includes all questions on the previous database with additional questions relating to training and risks.

These include all questions asked as part of the Data Assurance Corporate Records Audit that had been undertaken in previous years and focussed on a small number of key systems including ESR (HR), SystmOne (clinical records), R4 (dental), payroll and finance systems.

In addition to the twice yearly IAOs meeting, monthly IAO/IAAs workshops/meetings take place. These are an opportunity to discuss developments with the system, propose changes and to ask questions or raise issues.

The Information Asset Register and associated bulk flow data help 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, applications, and system software etc. There are currently (as of 22 June 2023) 147 Information Assets operating across the Trust and recorded on the Information Asset Register. Where risks are identified associated with an asset, these are placed on the relevant risk register and monitored by the IGG.

### 4.2 Information Asset Owners and Administrators

The responsibilities and accountabilities of IAOs are to:

- understand and address risks to the information asset they ‘own’.
- ensure policies and procedures are followed.
- recognise potential or actual security incidents.
- complete annual training for IAO/IAAs
- be accountable to the SIRO to provide assurance on security and use of these assets.

The responsibilities and accountabilities of IAAs are to:

- ensure policies and procedures are followed.
- recognise potential or actual security incidents.
- complete annual training for IAO/IAAs
- consult their IAO on incident management and
- ensure that information asset registers are accurate and up to date.

As of June 2023, the Trust identified 47 IAOs and 74 IAAs.

### 4.3 Organisations and Contractors

As of June 2023, The Records Manager and Data Protection Manager together with the IAOs have identified 42 organisations or contractors with whom we share information. Work is ongoing to ensure the Trust has either a contract or an up-to-date information sharing agreement (ISA) with each organisation or contractor.

### 4.4 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 actively managed, monitored and have up to date actions against them.

### 4.5 Data Protection Impact Assessments (DPIA)

The DPIA Group meets every 2 weeks to consider privacy risks associated with the implementation of new information assets or changes to existing assets. In 2022/2023 the group considered 36 DPIAs, of these:

- 25 were approved.
- 2 were denied.
- 4 were still pending.
- 4 were returned, awaiting further information.
- 1 was withdrew.

### 4.6 Information Security

Data security is actively managed by both the Information Governance and Cyber Security teams within Digital Services which forms the information security function within Digital Services.

Information governance and data security risks are monitored by the Information Governance Group (IGG) and are included in the DPST assessment. The IGG reports to the Digital Steering Group (DSG), to the Senior Leadership Team and the Executive Management Team meetings on a regular basis. The Cyber Security Team reports fortnightly to the Chief Information Officer (CIO)/SIRO identifying events, actions and any security enhancements made to progress the security targets set by the Trust. Any high-risk breach or incident are reported to the Risk and Compliance Group, the Senior Management Team and up to the Board, by exception.

Weekly CareCERT bulletins and ad hoc CareCERT notifications are promptly acted upon, risks identified and escalated appropriately, with immediate remediation work scheduled when necessary. A weekly traffic light status of Red/Amber/Green is kept up to date every Friday.

The Cyber Security Team continually implement new cyber defences and has expanded automated monitoring systems. 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 since 2018.

The Trust complies with the requirements of the Cyber Essentials Plus scheme being last certified on the 11th of September 2021, and following a gap analysis in March 2023 the renewal of the Cyber Essential Plus is due for completion by this Autumn.

The team has also maintained its engagement in partnership with local, regional, and national trusts and organisations in tackling system-wide attacks which enhances the security of our system. This includes active participation to the Yorkshire and Humber WARP (Warning, Advise and Reporting Point) as well as in the national Cyber Associate Network (CAN). This enables collaborative processes in taking both proactive steps and reactive actions affecting regional/national systems.

### 4.7 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 has Information Sharing Agreements with many partners.

The Clinical System Access Group has considered 101 requests from other partners to access the Trust's clinical systems, of these:

- 58 were approved.
- 5 are awaiting review.
- 28 were rejected.
- 6 are currently being reviewed.
- 4 were returned awaiting further information.

The IG Team is fully engaged within the Act as One programme of work within Bradford District and Craven, co-leading the IG workstream, a key enabler for cross agencies information sharing across Place.

### 4.8 Freedom of Information Requests (FOI)

During 2022/23, the Trust received a total of 453 requests under the Freedom of Information Act. 329 requests were managed within the twenty working day timescale (78%).

### 4.9 Requests for Personal Information

During 2022/23 the Trust received 662 requests for personal information 286 of which were Subject Access Requests (SARS) and 376 were Third Party Requests (TPRs).

### 4.10 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 296 (96%) were responded to within the required timescale.

### 4.11 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. 95% of the 391 Third Party Requests completed in this period were responded to within 40 days.

### 4.12 Paper Records

Whilst the Trust has few paper records or documents in active use (limited dental records, district nursing records to be left at a Service Users home and some inpatient forms), these are decreasing in number. However, we do need to keep clinical, personnel and corporate.

paper records for periods laid down in the relevant retention schedules. The majority of records are held by the IG team using a commercial storage company. There are currently (as of June 2023) 21,400 boxes held in this facility. Until October 2022 there was a moratorium on destruction of records as the Independent Inquiry into Child Sexual Abuse had advised all public bodies that they may require records as part of their enquiries. With the conclusion of the Inquiry in October 2022 the IG team has re-commenced the destruction of records were

they have reached their destruction period. There is also the Covid Inquiry, which is ongoing, and where we have a requirement to retain records that may be required; however, these records will be electronic rather than older paper ones. The destruction of relevant paper records and reduction in total holdings will continue in 2023/24.

During 2022/23 there has also been a large push to remove all paper records from Trust sites. This has included all records held at New Mill. The New Mill records have included thousands of pensions and payroll records which need to be retained until the staff member reaches 75 years of age. These records have been scanned meaning all of the paper records have been able to be destroyed. This work is good IG practice and helps the supports the Trust's estate strategy and net carbon objectives.

### 4.13 Staff Awareness Survey and Home Audit

During 2022/23 BDCFT staff have taken part in an IG awareness survey and home and mobile workers have completed self-audits (both via Microsoft Teams). Both the survey and audit have shown high levels of data security and confidentiality awareness. The results have been used to tailor training and guidance.

## 5 Summary of Key Achievements in 2022/23

5.1 The following were achieved during 2022/23 in relation to Information Governance:

- review and analysis of the DSPT, including.
  - full compliance with the mandatory requirements of the DSPT
  - completion of the actions in the Information Governance internal audit plan
  - no serious incidents recorded on the DSPT.

- review 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 policy (BOYD)
  - Recording of Staff by Service Users etc policy
  - Acceptable use policy
  - Printing policy
  - Clinical Systems Security policy
  - CCTV policy

- New Privacy Notice
- Reviewed and revised the IG Staff handbook.
- further embedding of information governance awareness through the IG staff survey results
- fundamental review and update of the Information Asset Register and bulk data flows with the creation and introduction of a new digital in-house solution
- completion of the Data Assurance and Corporate Records Audit
- completion of the IGG workplan.
- regular scrutiny of information governance performance through the IG dashboard
- introduction of additional information security assurances
- 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.
- embedded the Clinical Systems Access Review Group and underlying process to ensure new requests for clinical systems access are streamline and documented.
- review and update of the IG pages on the SharePoint site
- supported the Trust with its move towards the sharing out of clinical records via the Tasking and Sharing project.
- Carried out an IG staff awareness survey and conduct a home/mobile worker IG audit.
- Reduction of overall paper holdings of the Trust in line with record retention schedules and good data protection principles

## 6 Plans for 2023/24

6.1 The following Information Governance objectives are to be considered for 2023/24:

- to meet all new and existing standards within the DSPT
- Cyber Essentials plus re-certification
- introduction of Cyber Assurance Framework requirements within the Trust digital strategy and DSPT requirements
- 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 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 Data Protection and Digital Information (No. 2) Bill 2022-23
- 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 embed the Data Security staff survey
- 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 on a monthly basis
- 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 Place.
- to support the Trust to enhance integrated working across the Bradford District and Craven Place and the Act as One programme of work.
- to understand and embed any new requirements to support the Trust to comply with the NHSX IG Framework.
- Carry out further IG home/mobile worker audit:
- Carry out further IG staff awareness survey.
- Continue process of reducing the Trusts overall paper records holdings.

## 7 Recommendations:

That Board:

- note the assurances provided in the paper; and
- note the proposed information governance objectives for 2023/2024.

## 8 Legal and Constitutional

None identified. The Trust acknowledges the importance of demonstrating good practice against information governance standards and compliance with the Data Security and Protection toolkit.

## 9 Quality and Compliance

None identified. The Trust acknowledges the importance of demonstrating good practice against information governance standards and compliance with the Data Security and Protection toolkit.

## 10 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/ Gaynor Toczek**
**Title / Data Protection Officer**
**Date paper / June 2023**

**Appendices 1**

| **Breach Type** | |
|---|---|
| **Availability** | |
| Corruption or inability to recover electronic data | 15 |
| Unauthorised or accidental loss | 387 |
| Denial of Service (Not Cyber) | 45 |
| Lost or stolen paperwork | 8 |
| Lost in Transit | 9 |
| Loss or stolen unencrypted device | 0 |
| Lost or Stolen Hardware | 38 |
| Loss or theft of only copy of encrypted data | 0 |
| Data left in insecure location | 23 |
| 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 | 94 |
| Phishing emails | 0 |
| Data sent by email to incorrect recipient | 31 |
| Uploaded to website/intranet in error | 2 |
| Unauthorised upload to social media | 1 |
| Data posted or faxed to incorrect recipient | 54 |
| Unauthorised access/disclosure | 34 |
| Spoof website | 0 |
| Failure to redact data | 1 |
| Cyber bullying | 0 |
| Verbal disclosure | 7 |
| Failure to use bcc when sending email | 3 |
| Cyber security misconfiguration (e.g., inadvertent publishing of data on website; default passwords) | 0 |
| Hacking | 2 |
| Cyber incident (key logging software) | 0 |
| **Integrity** | |
| Unauthorised or accidental alteration | 1 |
| Website defacement | 0 |
| Cyber incident unknown | 1 |
| Other | 11 |
| Total | 768 |

**Appendices 2**

**Key responsibilities of the Senior Information Risk Owner**

The key responsibilities of the SIRO include:

- overseeing the development of 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.

**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:

- reviewing and monitoring of the Trust's compliance with the Data Security and Protection Toolkit (DSPT).
- reviewing and monitoring of the Trust's annual Information Governance Strategy and Plan.
- reviewing and monitoring of any information governance risks, ensuring appropriate escalation to the Board.
- reviewing 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 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. Data Protection Impact Assessment (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.

**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:

- **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.

- **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.

- **Training:** All staff complete appropriate annual data security training and pass a mandatory test.

- **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.

- **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.

- **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.

- **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.

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

- **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.

- **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.