

## Meeting of the Board of Directors - **Public**

**08 July 2021**

<b>Paper title:</b>	Annual Report by the Senior Information Risk Owner (SIRO)	<b>Agenda item</b>  <b>25</b>
<b>Presented by:</b>	Tim Rycroft, Associate Director of Informatics / CIO / SIRO	
<b>Prepared by:</b>	Gaynor Toczek, information Governance & Records Manager / Data Protection Officer	

Purpose of the report		
This annual report by the Senior Information Risk Owner (SIRO) 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.	For approval	
	For discussion	
	For information	√

Executive summary		
<b>This annual report documents:</b>		
<ul style="list-style-type: none"> <li>• 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)</li> <li>• Informs the Board of information security risk assessments and details compliance with the Data Security and Protection Toolkit 2020/21.</li> <li>• Provides assurance of ongoing improvements in the relation to managing risks to information.</li> <li>• Details any Serious Incidents relating to personal data or breaches of confidentiality.</li> <li>• Outlines the direction of information governance work for 2021/22</li> </ul>		
Do the recommendations in this paper have any impact upon the requirements of the protected groups identified by the Equality Act?	<b>State below</b> <b>'Yes' or 'No'</b>  <b>No</b>	If yes please set out what action has been taken to address this in your paper

Recommendation
<p>The Board of Directors is asked to:</p> <ul style="list-style-type: none"> <li>• consider the information and assurances provided for 2020/21</li> <li>• note the proposed information governance objectives for 2021/22</li> </ul>

<b>Strategic vision</b>				
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

<b>Care Quality Commission domains</b>				
Please mark those that apply with an X				
Safe	Effective	Responsive	Caring	Well Led
X		X		X

<b>Relationship to the Board Assurance Framework (BAF)</b>	The work contained with this report links to the following strategic risk(s) as identified in the BAF: <ul style="list-style-type: none"> <li>Information Governance / Cyber Security supports and underpins the strategic risks for the Trust.</li> </ul>
<b>Links to the Supporting Operational Risk Register</b>	The work contained with this report links to the following corporate risk(s) as identified in the Supporting Operational Risk Register: <ul style="list-style-type: none"> <li>2046 / 2207</li> </ul>
<b>Compliance and regulatory implications</b>	The following compliance and regulatory implications have been identified as a result of the work outlined in this report: <ul style="list-style-type: none"> <li>Data Protection Act 2018</li> <li>Freedom of Information Act 2000</li> <li>General Data Protection Regulation 2018</li> <li>Data Security and Protection Toolkit</li> </ul>

## Annual Report 2020/21 - 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

The Information Governance Group (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:

- Information Governance Policy.
- Confidentiality and Data Protection Policy.
- Freedom of Information Policy.
- Records Management Policy.
- Information Security Policy.
- Clinical Systems Data Quality Policy.
- Clinical Information Systems Security Policy
- Risk Management Policy.
- Incident Management Policy.
- Social Media Policy.
- Employment Policy includes the
  - Mandatory and Required Training policy.
  - Registration Authority Policy.

### **1.3 Data Security and Protection Toolkit (DSPT)**

The Data Security and Protection Toolkit 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, provided linked to the revised Information Governance Toolkit
- **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

## 2. Status of Organisational Compliance

### 2.1 DSPT 2020/21

To be compliant with the toolkit in 2020/21 all evidence marked as “mandatory” needs to have been met. There are 110 mandatory evidence items in total underpinning 42 assertions.

An ‘Assurance level based on the confidence level of the Independent Assessor in the veracity of the self-assessment’ as ‘High’.

Due to the late publication of the DSP Toolkit to organisations, the deadline was extended until the end of June 2021.

The DSP assessment was submitted 15/06/2021 as **Standards Exceeded**.

### 2.3 Internal audit

During 2020/21 Audit Yorkshire conducted an audit of the Data Security and Protection Toolkit and IT Security for which the Trust gained **High assurance**.

The auditor identified 3 significant findings and provided recommendations, which the Trust has or is working towards addressing.

### 2.4 Serious Incidents Requiring Investigation (SIRI) in 20/21

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 within 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.

Between 1 April 2020 and 31 March 2021 there were 450 IG incidents reported on the Trust's incident Management system, as shown below. There was 1 incident recorded as a SIRI. This was logged on the Trust's Serious Incident system and reported to the Information Commissioner's Office (ICO) via the DSPT portal.

#### Summary of Data Security and Protection Incident reported to the ICO and/or DHSC.

Date of incident	Nature of incident	Number affected	How patients were informed
March 2021	157 letters copied to an incorrect service: A letter informing parents and school nurses that a referral to CAMHS was being redirected to another service should have advised that a copy be sent to the school nurse, had inadvertently been changed to "school".	157	Duty of Candour letter sent by the Medical Director to all those affected on the 29 <sup>th</sup> of April 2021.

The ICO were satisfied with the action the Trust had taken and consider the matter closed. The ICO did provide some recommendations which the Trust had already acted upon or were considering.

## 2.5 Incidents reported in 2020/21

<b>Summary of Other Personal Data Related Incidents in 2020/21</b>	
<b>Breach Type</b>	<b>Total</b>
<b>Availability</b>	
Corruption or inability to recover electronic data	4
Unauthorised or accidental loss	0
Denial of Service (Not Cyber)	26
Lost or stolen paperwork	18
Lost in Transit	9
Loss or stolen unencrypted device	0
Lost or Stolen Hardware	16
Loss or theft of only copy of encrypted data	0
Data left in insecure location	17
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	2
<b>Confidentiality</b>	
Disclosed in Error	47
Phishing emails	7
Data sent by email to incorrect recipient	40
Uploaded to website/intranet in error	2
Unauthorised upload to social media	3
Data posted or faxed to incorrect recipient	50
Unauthorised access/disclosure	31
Spoof website	0
Failure to redact data	1
Cyber bullying	2
Verbal disclosure	7
Failure to use bcc when sending email	8

Cyber security misconfiguration (e.g., inadvertent publishing of data on website; default passwords)	0
Hacking	1
Cyber incident (key logging software)	0
<b>Integrity</b>	
Unauthorised or accidental alteration	0
Website defacement	0
Cyber incident unknown	0
Other	159
<b>Total</b>	<b>450</b>

### 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 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 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 Manager has identified 146 Information Assets operating across the Trust. Where risks are identified in associated with an asset, this is 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 2020, the Trust had identified 44 IAOs and 99 IAAs.

### **3.3 IAO and IAA Training Compliance**

As a minimum the Trust requires that IAOs and IAAs complete the “NHS Information Risk Management for SIROs and IAOs” refresher module annually. This has previously been a combination of online and predominantly classroom-based delivery by the Trust Head of IG. Due to the limitations of classroom delivery this past year, further reliance via online training has been relied upon.

At the end of March 2021, 23% of IAOs and 9% of IAAs were compliant with this training requirement. This is based on the data extracted from ESR which requires some further cleansing and therefore is expected to under-represent the true position.

All IAOs and IAAs have completed their mandatory annual IG training.

### **3.4 Organisations and Contractors**

The Information Governance and Records Manager, together with the IAO's has identified 341 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. A review of all ISAs commenced in April 2018 and is now business as usual.

### **3.5 Information Governance Risks**

During 2020/21 the Trust had 3 information governance risks on its local 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 has also achieved Cyber Essential Plus in September 2020, ahead of the national deadline of June 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 Bradford Inter-agency Information Sharing Protocol which is currently under review at Bradford District and Craven level, in which the Trust actively contribute and has Information Sharing Agreements with many partners.

### **3.8 Freedom of Information Requests (FOI)**

During 2020/21, the Trust received a total of **328** requests under the Freedom of Information Act. **228** requests were managed within the twenty working day timescale, and **78** responses were not managed within the FOI timescales.

### **3.9 Requests for Personal Information**

During 2020/21 the Trust received **622** requests for personal information **281** of which were Subject Access Requests (SARS) and **341** 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 one calendar month from date of receipt. Correct and prompt management of subject access requests 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 **243 (92%)** 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. **96%** of the **321** 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 Records Management 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 2020/21:

- SystemOne (clinical)
- Safeguard (Complaints, Litigation, and Incident Management)

- ESR (Workforce)
- Oracle (Finance)
- Payroll/ESR
- R4 (Clinical – Dental)

3 potential risks were identified.

#### **4. Summary of Key Achievements in 2020/21**

4.1 The following were achieved during 2020/21 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 1 Level SIRI recorded on the DSPT.
- completion of all actions in the revised Caldicott Plan.
- 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
  - Data Quality policy
  - Clinical Information Systems policy
- 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 and IT Security.
- regular scrutiny of information governance performance through the IG dashboard.
- introduction of additional IG security assurances.
- gained cyber essentials plus certification.
- review and approval of key information governance strategies and plans, including.
  - Information Governance Strategy
  - Information Governance Training Strategy

- Information Asset Register Delivery Strategy
- strengthened governance processes with IAOs and IAAs.
- thorough reorganisation of archived records processes
- reviewed and embedded the Data Protection Impact Assessment (DPIA) process
- thorough review of Information Sharing Agreements
- creation of Clinical Systems Access review group and underlying process to ensure new requests for clinical systems access are streamline and documented for a maximum of 12 months.

## 5. Plans for 2021/22

5.1 The following Information Governance objectives are to be considered for 2021/22:

- 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.
- 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 further understand and embed the requirements of the General Data Protection Regulation (GDPR) 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 6-monthly meetings
- to improve compliance with IAO/IAA training levels.
- to review the Information Asset Register and Bulk Data flows collection to ensure compliance with new legislation.
- to embed the new Data Security staff survey.
- to ensure the Trust is in full compliance with the Jay (Goddard) 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 review the use of honorary contracts.
- to investigate the implications of the National Data, Opt-Out.
- to further enhance the IG and Cyber Security dashboard.
- To progress use of the Information Sharing Gateway as a register for information sharing agreements and explore the gateway to capture data protection impact assessments.

The next Annual Report to the SIRO will be produced in May 2022.

## 6. Recommendations:

That the IGG:

- note the assurances provided in the paper; and
- note the proposed information governance objectives for 2021/22.

## 7. Implications

### 7.1 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.

### 8. 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.

### 9. Risk Issues Identified

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



Gaynor Toczek Information Governance and  
Records Manager/Data Protection Officer  
14/06/2021