Bradford District Care
NHS Foundation Trust

PUBLIC TRUST BOARD MEETING

30 May 2019

Paper Title:	Annual Report by the Senior Information Risk Owner (SIRO)
Lead Director:	Tim Rycroft, Associate Director of Informatics and SIRO
Paper Author:	Gaynor Toczek, Information Governance & Records Manager / DPO
Agenda Item:	**Item - 16**
Presented For:	Assurance
Paper Category:	Governance & Compliance

Executive Summary:

This annual report by the Senior Information Risk Owner (SIRO) represents good practice that the Board receives a written annual report of this nature. The report covers the period 1 April 2018 to 31 March 2019 and is intended to:

a) document 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);

b) inform the Board of information security risk assessments and approve identified risk mitigation plans if required;

c) detail compliance with the Data Security and Protection Toolkit 2018/19;

d) provide assurance of ongoing improvements in the relation to managing risks to information;

e) detail any Serious Incidents Requiring Investigation relating to any losses of personal data or breaches of confidentiality; and

f) outline the direction of information governance work for 2019/20 and how this aligns with the strategic business goals.

Recommendations:

That the Board

- To consider the information and assurances provided for 2018/19
- note the proposed information governance objectives for 2019/20.

Governance/Audit Trail:

Meetings where this item has previously been discussed (*please mark with an X):*							
Audit Committee		**Quality & Safety Committee**		**Remuneration Committee**		**Finance, Business & Investment Committee**	
Executive Management Team		**Directors**		**Chair of Committee Meetings**		**Mental Health Legislation Committee**	
Council of Governors							

This report supports the achievement of the following strategic aims of the Trust: (*please mark those that apply with an X):*	
Quality and Workforce: to provide high quality, evidence-based services delivered by a diverse, motivated and engaged workforce	
Integration and Partnerships: to be influential in the development and delivery of new models of care locally and more widely across West Yorkshire and Harrogate STP	X
Sustainability and Growth: to maintain our financial viability whilst actively seeking appropriate new business opportunities	X

This report supports the achievement of the following Regulatory Requirements: (*please mark those that apply with an X):*	
Safe: People who use our services are protected from abuse and avoidable harm	
Caring: Staff involve people who use our services and treat them with compassion, kindness, dignity and respect	
Responsive: Services are organised to meet the needs of people who use our services	
Effective: Care, treatment and support achieves good outcomes, helps to maintain quality of life people who use our services and is based on the best available evidence.	
Well Led: The leadership, management and governance of the organisation make sure it's providing high-quality care that is based around individual needs, encourages learning and innovation, and promotes an open and fair culture.	X
NHSI Single Oversight Framework	X

Equality Impact Assessment:
Nothing to report.

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

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 Informatics Board 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 Information Governance Toolkit;
- review and monitoring of the Trust's annual Information Governance 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 Information Governance Toolkit;

- reviewing all information governance policies and procedures;
- monitoring trends from incident reporting; and
- 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;
- Registration Authority Policy;
- Information Security Policy;
- Data Quality Policy;
- Clinical Systems Policy;
- Risk Management Policy;
- Incident Management policy;
- Consent Policy;
- Social Media Policy;
- BYOD and Acceptable Use Policy and
- Mandatory and Required Training policy.

1.3 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 DSP Toolkit 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.

In order 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.

1.4 Data Security and Protection Toolkit (DSP)

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 DSP Toolkit 2018/19

To be compliant with the toolkit in 2018/19 all evidence marked as "mandatory" needs to have been met. There were 100 mandatory evidence items in total underpinning 40 assertions.

The DSP assessment was submitted 28/03/2019 as **Standards Met**.

2.3 Internal audit

During 2018/19 Audit Yorkshire conducted an audit of Data Security and Protection Toolkit and IT Security for which the Trust gained **significant assurance**.

16 recommendations were raised following this review. Only 2 remain to be actioned. The suggested deadline for completion is October 2019.

2.4 Serious Incidents Requiring Investigation (SIRI) in 2018/19

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. From May 2018 it is a legal obligation to notify personal data breaches of the General Data Protection Regulation under Article 33 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 2018 and 31 March 2019 there were 401 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 (month)	Nature of incident	Number affected	How patients were informed
20 November 2018	Patient's partner was able to listen to a staff discussion due to being accidently called back on staff mobile phone.	3	Team leader spoke to the patient and apologised.

2.5 Incidents reported in 2018/19

Summary of Other Personal Data Related Incidents in 2018/19		
Category	**Breach Type**	**Total**
Availability		
Corruption or inability to recover electronic data		44
Unauthorised or accidental loss		5
Denial of Service (Not Cyber)		118
Lost or stolen paperwork		23
Lost in Transit		5
Loss or stolen unencrypted device		0
Lost or Stolen Hardware		18
Loss or theft of only copy of encrypted data		0
Data left in insecure location		9

Cyber incident (other DDOS etc)	1
Cyber incident (exfiltration)	0
Cryptographic flaws (e.g. failure to use HTTPS; weak encryption)	0
Non-secure disposal – hardware	1
Malicious internal damage	0
Non-secure disposal – paperwork	6
Confidentiality	
Disclosed in Error	61
Phishing emails	3
Data sent by email to incorrect recipient	13
Uploaded to website/intranet in error	3
Unauthorised upload to social media	1
Data posted or faxed to incorrect recipient	40
Unauthorised access/disclosure	27
Spoof website	0
Failure to redact data	1
Cyber bullying	2
Verbal disclosure	8
Failure to use bcc when sending email	4
Cyber security misconfiguration (e.g. inadvertent publishing of data on website; default passwords)	0
Hacking	3
Cyber incident (key logging software)	0
Integrity	
Unauthorised or accidental alteration	0
Website defacement	0
Cyber incident unknown	0
Other	5

3. Risk Management and Assurance

3.1 Information Assets

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 133 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;
- recognises potential or actual security incidents;
- consult their IAO on incident management; and
- ensure that information asset registers are accurate and up to date.

As at November 2018 the Trust had identified 35 IAOs and 74 IAAs.

3.3 IAO and IAA Training Compliance

IAOs and IAAs have been reminded of their training requirements as part of the IG communications plan. At present the only option available for staff to complete training is via the IAO's biannual meeting, this is due to the withdrawal of the national online IAO IG training tool. There was only one meeting between the IAOs/IAAs and SIRO in 2018/19. This was the only opportunity for the IAOs and IAAs to update their training compliance, strengthen their governance role and awareness.

Therefore, at the end of 2018/19, only 8 of the 35 IAOs were in date with their required training (23%), and 10 of the 54 IAAs were in date with their required training (19%). Note: 20 of the 74 IAAs are also IAOs, these statistics count individuals and not assets.

In terms of mitigation all IAO/IAA's have completed their respective mandatory IG training which provides an acceptable level of awareness regarding their resposnbilites.

3.4 Organisations and Contractors

The Information Governance and Records Manager together with the IAOs has identified 36 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 part of an ongoing process.

3.5 Information Governance Risks

During 2018/19 the Trust had 5 information governance risks on its local Risk Register, 2 of which were closed and archived in year.

All live risks are monitored and have actions against them. Existing risks include monitoring of contracts and SLAs in line with GDPR, embedding "Privacy by Design" and resources for delivering requests by statutory deadline.

3.6 Information security

During the course of the year the IGG has considered a number of data security/cyber security issues in the light of increased incidents of phishing and spam alerts monitored by the Informatics Department. There is now a comprehensive, approved cyber security plan introducing a 6 -monthly report on cyber security to the IGG and weekly updates to the Senior Informatics team, including the SIRO.

Communications are distributed to staff to raise awareness of cyber security issue.
The Cyber security team continue to work towards the attainment of Cyber Essential Plus, which will become a mandated requirement for all NHS organisations by 2020.

Communications are distributed to staff to raise the awareness of cyber security threats. The Trust Board also received cyber awareness training in November 2018, this was a sponsored activity by NHS Digital to ensure that cyber risks are understood at Board level.

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 Interagency Information Sharing Protocol.

3.8 Freedom of Information Requests (FOI)

During 2018/19, the Trust received a total of **428** requests under the Freedom of Information Act. **369** were managed within the twenty working day timescale, and **59** responses were not managed within the FOI timescales.

3.9 Requests for Personal Information

During 2018/19 the Trust received **538** requests for personal information **287** of which were Subject Access Requests (SARS) and **242** 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 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 **266 (93%)** 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. 86% of the 242 Third Party Requests completed in this period were responded to within 40 days.

	SARs	**TPRs**
Completed	287	242
Completed within 40 days	266	207

3.12 Data Assurance Framework

In keeping with the principles of the Data Protection Act (2018) the Trust has a Data Assurance Framework. This provides BDCFT with a bi-annual update on progress regarding:

- review of data quality;
- internal data assurance processes; and
- formal data assurances via internal and external audit.

Quality data supports the delivery of quality patient care through effective service delivery, improved patient experience and patient safety. For data to be used as a foundation for decision making and delivering quality patient care it must be accurate, complete, reliable, appropriate and accessible at the point of care. The Trust must satisfy a series of due diligence requirements, of which assurance of data quality in clinical systems is a key requirement. The Trust is committed to supporting the production of quality data and information to support the delivery of quality patient care.

4. Summary of Key Achievements in 208/19

4.1 The following were achieved during 2018/19 in relation to Information Governance:

- review and analysis of the new Data Protection and Security Toolkit;
- compliance with the requirements of the Data Security and Protection Toolkit;
- completion of the actions in the GDPR Readiness plan
- continued information governance compliance site audits conducted across the Trust;
- only 1 Level SIRI recorded on information governance-related issues;
- completion of all actions in the revised Caldicott Plan;
- review and ratification of a number of 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
    - Clinical Information System Data Quality policy
    - Clinical Information Systems policy
    - Consent 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
- significant audit assurance for Data Security and Protection Toolkit and IT Security
- regular scrutiny of information governance performance through the IG dashboard;
- introduction of additional IG security assurances;
- review and approval of key information governance strategies, including;
    - Information Governance Strategy
    - Information Governance Training Strategy

    - Information Asset Register Delivery Strategy
- strengthened governance processes with IAOs and IAAs through 6-monthly meetings and face to face training.

5. Plans for 2018/19

5.1 The following Information Governance objectives are to be considered for 2019/20:

- to continue meet all standards within the Data Security and Protection Toolkit;
- 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);
- to further understand and embed the requirements of the new General Data Protection Regulation (GDPR);
- to further understand and embed the requirements of the new Data Protection Bill (DPA 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 by offering on-line training;
- to review the Information Asset Register and Bulk Data flows collection to ensure compliance with new legislation;
- to monitor and review the effectiveness of IG&RM communications via the annual IG&RM survey;
- 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 introducing a new clinical information system for mental health services;
- to review cyber security incidents on a monthly basis
- to develop a monthly Dashboard for cyber security to be presented at IGG;
- to escalate any risks or areas of concern to the Informatics Board 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.
- Training for IAOs and IAAs will be available via the Electronic Staff Record (ESR) system throughout 2019/20 which will enable improvement in training compliance.

The next Annual Report to the SIRO will be produced in May 2020.

6. Recommendations:

That the Board:

- note the assurances provided in the paper; and
- note the proposed information governance objectives for 2019/20.

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
Non-compliance with information governance requirements operating as an FT.	Low	Reputational damage and potential financial consequences imposed by regulators.	Existing governance arrangements (Informatics Board and Information Governance Group) and risk escalation processes.