Bradford District Care NHS
NHS Foundation Trust

PUBLIC BOARD MEETING

25 May 2017

Paper Title:	Annual Report by the Senior Information Risk Owner (SIRO)
Lead Director:	Paul Hogg, Trust Secretary and SIRO
Paper Author:	Gaynor Toczek, Information Governance and Records Manager
Agenda item:	**16**
Presented for:	Information/assurance

1. Purpose of this Report:

This is the second written annual report by the Senior Information Risk Owner (SIRO). It is good practice that the Board receives a written annual report of this nature. The report covers the period 1 April 2016 to 31 March 2017 and is intended to:

- document compliance with legislative and regulatory requirements relating to the handling of information, including compliance with the Data Protection Act (1998) and the Freedom of Information Act (2000);
- inform the Board of information security risk assessments and approve identified risk mitigation plans if required;
- detail compliance with the Information Governance Toolkit 2016/17;
- provide assurance of ongoing improvements in the relation to managing risks to information;
- detail any Serious Incidents Requiring Investigation (SIRI) relating to any losses of personal data or breaches of confidentiality; and
- outline the direction of information governance work for 2017/18 and how this aligns with the strategic business goals.

2. Summary of Key Points

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.

3. Board consideration

To consider the information and assurances provided for 2016/17 and note the proposed information governance objectives for 2017/18.

4. Financial Implications

None identified as a result of this paper. Approval of resources to support information governance is addressed through regular annual planning discussions.

5. Legal Implications

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

6. Assurance

	Assurance provided?
Board Assurance Framework	Yes
CQC Themes (see below)	Yes
Single Oversight Framework	Yes
Other (please specify):	

This paper provides assurance in relation to the following CQC Key Question:

Well led:	Do 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?

6. Equality Impact Assessment

Not applicable.

7. Previous Meetings/Committees Where the Report Has Been Considered:

Audit Committee	□	Quality & Safety Committee	□	Remuneration Committee	□	FB&I Committee	□
Executive Management team	☒	Directors Meeting	□	Chair of Committee's Meeting	□	MH Legislation Committee	□

Assurance papers underpinning this report have been submitted to the committees identified above.

8. Risk Issues Identified for Discussion

Risk	Likelihood	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.

9. Links to Strategic Drivers

Patient Experience	Quality	Value for Money	Relationships
Effective use of information governance is relevant to all four Strategic Drivers.			

10. Publication Under Freedom of Information Act

This paper has been made available under the Freedom of Information Act.

11 . Recommendations:

That the Board:

- note the assurances provided in the paper; and
- note the proposed information governance objectives for 2017/18.

Annual Report by the Senior Information Risk Owner (SIRO)

1. Information Governance Background

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; 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 IG Toolkit submission in March each year. The collection and risk assessment also serves 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 Information Governance Toolkit

The Information Governance Toolkit is an online tool that enables organisations to measure their performance against a set of information governance requirements, including the following:

- Information Governance Management;
- Confidentiality and Data Protection Assurance;
- Information Security Performance;
- Clinical Information Assurance;
- Secondary Users Assurance; and
- Corporate Information Assurance.

There are 3 assessments annually:

- Baseline 31 July;
- Performance Update 31 October; and
- Final Submission 31 March.

2. Status of Organisational Compliance

2.1 IG toolkit 2016/17

The final submission of the IG Toolkit was submitted at the end of March 2017 and the Trust was compliant with the requirements of the toolkit and all requirements were at level 2 or above:

Level 0	Level 1	Level 2	Level 3	*Not Applicable	Total no. of Requirements	% Score
0	0	10	34	1	45	92%

2.2 Information Commissioner's Office

In October 2015, the Trust was audited by the Information Commissioner's Office (ICO), which reviewed two strands of the Data Protection Act around data protection governance and data sharing systems and processes. During 2016/17, the Trust received a report on the positive outcome of the Information Commissioners Office's (ICO) desk top review in December 2016, following the consensual audit undertaken in October 2015. The review measured the extent to which the Trust had implemented the agreed recommendations on two strands of the Data Protection Act. Delivery of the action plan was coordinated by the Information Governance team, overseen by the IGG and reported to Audit Committee. The ICO acknowledged the significant progress made against the scoped areas, having completed 26 of the 32 recommendations made in the original report at the time of the review and now consider the audit engagement complete. The IGG continues to monitor the remaining five actions as part of the rolling IGG work programme.

2.3 Internal audit

During 2016/17, Audit Yorkshire conducted three audits that related in some way to information governance or informatics, as follows:

- Information security (significant assurance);
- IT Local Service provider Exit (significant assurance); and
- Informatics capacity (significant assurance).

In 2015/16 there was a limited assurance report on IT Asset Management. During 2016/17, the IGG discussed and endorsed the introduction of revised guidance documents for both Trust staff and the Informatics team in response to internal audit recommendations, explaining the purchasing, recording and management of IT assets across the Trust.

2.4 SIRI Report (linked to the Annual Governance Statement)

Information governance incidents are reported internally through the web based incident reporting system (IR-e) and notified immediately to the Information Governance (IG) & Records Manager for logging on the Serious Incidents Requiring Investigation section of the Information Governance Toolkit and with the Trust's Serious Incident Lead where appropriate. Incident data is regularly reported to and monitored by the IGG. In 2016/17, 154 (at Level 1) were reported to the IG Toolkit and investigated. There were no cases at Level 2 logged on the Trust's Serious Incident system during 2016/17. The Trust reported no IG breaches to the Information Commissioner's Office (ICO) in the year 2016/17. Between 1 April 2016 and 31 March 2017 there were 180 IG incidents reported on HSCIC's incident management system. There were no incidents at level 2 or above for the period 2016/17, as shown below:

Level 0	110
Level 1	154
Level 2	0

2.5 Incidents reported at Level 1 in 2016/17

Summary of Other Personal Data Related Incidents in 2016/17		
Category	**Breach Type**	**Total**
A	Corruption or inability to recover electronic data	1
B	Disclosed in Error	40
C	Lost in Transit	7

D	Lost or Stolen Hardware	1
E	Lost or stolen paperwork	90
F	Non-secure disposal - hardware	1
G	Non-secure disposal - paperwork	1
H	Uploaded to website in error	1
I	Technical security failing (including hacking)	0
J	Unauthorised access/disclosure	12
K	Other	0

2.6 Incidents at level 2 or above in 2016/17

There were no incidents at level 2 or above. When necessary, and in response to incidents, e-communications are developed and shared with all staff regarding the principles and practice of Information Governance.

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 108 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.

The Trust has identified 24 IAOs and 55 IAAs.

3.3 IAO and IAA Training Compliance

During 2016/17, 19 of the 24 IAOs were in date with their required training (79%), and 24 of the 55 IAAs were in date with their required training (44%). IAOs and IAAs have been reminded of their training requirements as part of the IG communications plan. There have been two meetings between the IAOs/IAAs and SIRO which updated training compliance, strengthened their governance role and awareness of IAOs and agreed a work programme for the forthcoming year.

3.4 Organisations and Contractors

The Information Governance and Records Manager together with the IAOs has identified 47 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 2016, and is now part of an ongoing process.

3.5 Information Governance Risks

During 2016/17 the Trust had 9 information governance risks on its local Risk Register, four of which were closed and archived in year. All live risks are monitored and have actions against them. Existing risks include generic areas such as the risk of IG breaches by staff, sanctions by the ICO if the organisation does not comply with its IG requirements, and risks associated with retrieval/storage of records relating the Jay (Goddard) Enquiry.

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. The Group supported the introduction of strengthened password standards documentation and requirements for staff to change their passwords more frequently; communications with staff to raise awareness of cyber security issues; and the introduction of a 6-monthly report on cyber security to the IGG (with quarterly updates direct to the SIRO).

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 Partnership Information Sharing Protocol.

3.8 Freedom of Information Requests (FOI)

During 2016/17, the Trust received a total of 375 requests under the Freedom of Information Act. 351 were managed within the twenty working day timescale, and 24 responses were not managed within the FOI timescales.

3.9 Requests for Personal Information

During 2016/17 the Trust received 385 requests for personal information 204 of which were Subject Access Requests (SARS) and 192 were Third Party Requests.

3.10 Subject Access Requests (SARS)

The Data Protection Act 1998, Section 7, 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 40 calendar days 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 204 SARs completed in this period 201 (99%) were responded to within the required 40 day timescale.

3.11 Third Party Requests (TPRs)

There is no statutory deadline for requests made by third parties (TPRs), however these are processed in the same way as SARs. 100% of the 192 Third Party Requests completed in this period were responded to within 40 days.

	SARs	TPRs
Completed	204	192
Completed within 40 days	201	192

3.12 Data Assurance framework

In keeping with the principles of the Data Protection Act (1998) 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 2016/17

4.1 The following were achieved during 2016/17 in relation to Information Governance:

- compliance with the requirements of the Information Governance toolkit;
- continued information governance compliance site audits conducted across the Trust;
- completion of the ICO action plan in readiness for the return desktop review;
- no Level 2 SIRIs recorded on information governance-related issues;
- approval of the revised Caldicott Plan;
- review of a number of key information policies, including the Clinical Data Quality policy, Clinical Information Systems policy, Confidentiality and Data Protection policy, Information Security policy and Freedom of Information policy;
- further embedding of information governance awareness through the IG staff survey results;
- regular scrutiny of information governance performance through the IG dashboard;
- introduction of additional IG security assurances;
- final review and completion of the 2014-2017 Information Governance Strategy;
- strengthened governance processes with IAOs and IAAs through 6-monthly meetings.

5. Plans for 2017/18

5.1 The following Information Governance objectives are to be considered for 2017/18:

- to continue to achieve Level 2 compliance against the Information Governance Toolkit and review the percentage of requirements achieving Level 3;
- to deliver a new training strategy for information governance and security management;

- to maintain zero serious untoward Information Governance Incidents (at Level 2);
- 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;
- to embed the new Records Management Code of Practice;
- to consider the implications of the new General Data Protection Regulations (GDPR);
- to continue to raise the profile of data sharing across the Trust and Health and Social Care;
- to engage IAOs/IAAs through 6-monthly meetings and improve compliance with IAO/IAA training levels;
- to monitor and review the effectiveness of IG&R communications via the annual IG&R survey.
- to ensure the Trust is in full compliance with the Jay (Goddard) Inquiry;
- to produce a revised Information Governance Strategy for 2017-2020;
- to review existing IG policies 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 6-mothly basis (with quarterly exception reports to the SIRO); and
- 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.

The next Annual Report will be produced in May 2018.

6. Recommendations:

That the Board:

- note the assurances provided in the paper; and
- note the proposed information governance objectives for 2017/18.