You and Your Care

Bradford District Care NHS
NHS Foundation Trust

PUBLIC BOARD MEETING

30 June 2016

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:	19
Presented for:	Information/assurance

1. Purpose of this Report:

This is the first written annual report by the Senior Information Risk Owner (SIRO). Previous reports have been verbal updates to the Information Governance Group. It is good practice that the Board receives a written annual report of this nature. The report 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 2015/16;
- 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 2016/17and 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.

The information submitted in this report has been considered by the Information Governance Group and the data presented in relation to information governance incidents was included in the 2015/16 Annual Report and Accounts.

3. Publication Under Freedom of Information Act

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

4. Recommendations:

That the Board:

- note the assurances provided in the paper; and
- note the information governance objectives for 2016/17.

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 is responsible for ensuring the effective management of the Trust's Information Governance processes and continues to meet bi-monthly. This group ensures the effective management of the Trust's Information Governance processes and provides information and assurance to the Technology Board quarterly about how risks are being managed within the organisation relating to Information Governance.

The key duties of the Information Governance Group include:

- Review and monitor the Trust's compliance with the Information Governance Toolkit;
- Review and monitor the Trust's annual Information Governance Plan;
- Review and monitor any Information Governance risks, ensuring appropriate escalation to the Board;
- Review and monitor new and changing information assets in compliance with the requirements of the Information Governance Toolkit;
- Review all Information Governance policies and procedures;
- Monitor trends from incident reporting; and
- Ensure 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 an on-line training module 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.

The October submission was audited by West Yorkshire Audit Consortium and this year's audit provided significant assurance. A further audit was undertaken relating to the final submission which also received a significant assurance rating.

2. Status of Organisational Compliance

2.1 IG toolkit 2015/16

The final submission of the IG Toolkit was submitted at the end of March 2016 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	11	33	1	45	91%

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. In completing the audit, the ICO found reasonable assurances for both separate elements and an overall conclusion of reasonable assurance. This was an excellent outcome for the Trust, one of the first health organisations to be audited by the ICO. A detailed report was produced by the ICO, supported by an action plan, summarising the 39 recommendations made. Delivery of the action plan is being coordinated by the Information Governance team, overseen by the Information Governance Group and reported to Audit Committee.

2.3 Internal audit

The Records Management Process gained significant assurance in a follow-up audit by West Yorkshire Audit Consortium in January 2016. The original audit took place in February 2015.

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 IG Group. In 2015/16, 69 (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 2015/16. The Trust reported no IG breaches to the Information Commissioner's Office (ICO) in the year 2015/16. Between 1 April 2015 and 31 March 2016 there were 180 IG incidents reported on HSCIC's incident management system. There were no incidents at level 2 or above for the period 2015/16, as shown below:

Level 0	120
Level 1	69
Level 2	0

2.5 Incidents reported at Level 1 in 2015/16

Summary of Other Personal Data Related Incidents in 2015/16		
Category	**Breach Type**	**Total**
A	Corruption or inability to recover electronic data	0
B	Disclosed in Error	25
C	Lost in Transit	3
D	Lost or Stolen Hardware	3
E	Lost or stolen paperwork	21
F	Non-secure disposal - hardware	0

G	Non-secure disposal - paperwork	1
H	Uploaded to website in error	0
I	Technical security failing (including hacking)	1
J	Unauthorised access/disclosure	14
K	Other	0

2.6 Incidents at level 2 or above in 2015/16

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. 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 Information Governance Group.

3.2 Information Asset Owners and Administrators

The responsibilities and accountabilities of Information Asset Owners 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 Information Asset Administrators 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 25 Information Asset Owners and 57 Information Asset Administrators.

3.3 IAO and IAA Training Compliance

During 2015/16, 20 of the 25 IAOs were in date with their required training: 80%; and 37 of the 57 IAAs were in date with their required training: 65%. Information Asset Owners and Administrators have been reminded of their training requirements as part of the IG communications plan. The first meeting of the IAOs and SIRO was held on 29 April 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 46 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, which will include a review of contracts.

3.5 Information Governance Risks

During 2015/16 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 Goddard Enquiry.

3.6 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.

3.7 Freedom of Information Requests (FOI)

During 2015/16, the Trust received a total of 268 requests under the Freedom of Information Act. 246 were managed within the twenty working day timescale, and 17 responses were not managed within the FOI timescales.

3.8 Requests for Personal Information

During 2015/16 the Trust received 528 requests for personal information 179 of which were Subject Access Requests (SARS) and 349 were Third Party Requests.

3.9 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 212 SARs completed in this period 208 (98%) were responded to within the required 40 day timescale.

3.10 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. 99% of the 281 Third Party Requests completed in this period were responded to within 40 days.

	SARs	TPRs
Completed	212	343
Completed within 40 days	208	340

3.11 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 2015/16

4.1 The following were achieved during 2015/16 in relation to Information Governance:

- Reasonable assurance achieved in a Data Protection Audit conducted by the Information Commissioner's Office (ICO);
- Significant assurance achieved in the annual IG Toolkit audit conducted by West Yorkshire Audit Consortium (WYAC);
- Significant Assurance achieved following a follow up audit of Records Management conducted by WYAC;
- Approval of a Privacy Impact Assessment (PIA) process to be used at the commencement of new projects;
- Ratification of a new Records Management Policy and procedures;
- A New Fair Processing Notice for service users approved by service user groups and surveys;
- Information Governance KPIs included in the recently approved Information Governance Group Dashboard;
- A new Terms of Reference (TOR) for this group was approved in January 2016. The TOR includes, revised membership and an annual work plan;
- Continued Information Governance compliance site audits conducted across the Trust;
- Complete revision and update to the Information Asset Register, together with a Bulk Data Flow assessment;
- New information sharing guidance for all staff; and
- Continued Information Governance face to face training delivered across the Trust.

5. Plans for 2016/17

5.1 The following Information Governance objectives have been agreed for 2016/17:

- Achievement of level 2 Information Governance Toolkit (Version 14). Maintain the percentage of requirements achieving level 3;
- Zero serious untoward Information Governance Incidents;
- Increase the percentage of Freedom of Information responses managed within the FOI timescales to 100% by quarter 4 2016/17;
- To continue to raise the profile of data sharing across the Trust and Health and Social Care.
- Review all Information Sharing Agreements and associated contracts;
- Monitor and review the effectiveness of IG&R communications via the annual IG&R survey.

- Ensure the Trust is in full compliance with the Goddard Inquiry;
- Implement the options chosen by EMT in regards to record retention;
- Implement a new Safeguard module for Freedom of Information Requests, and review suitability for Data Protection Act request;
- Complete ICO action plan in readiness for their review in December 2016;
- Full implementation of user-satisfaction surveys for all types of requests;
- A review of IG policies including:
  - Information Governance policy
  - Information Security policy
  - Confidentiality and Data Protection policy.
  - Freedom of Information policy
  - Records Management policy (minor review);
- Review of the Information Governance staff handbook;
- Review of IG and Records Management training materials;
- Review of IG procedures and guidance; and
- Introduction of 6-monthly meetings with IAOs.

The next Annual Report to the SIRO will be produced in May 2017.

6. Recommendations:

That the Board:

- note the assurances provided in the paper; and
- note the information governance objectives for 2016/17.