

**Board of Directors: 10.5.18**

**Agenda Item: Bo.5.18.11**

**Senior Information Risk Owner  
2017/18 Quarter 4 Update**

<b>Presented by:</b>	Cindy Fedell, Director of Informatics & Senior Information Risk Owner	<b>Author:</b>	Sandre Jones, Information Governance Consultant
<b>Previously considered by:</b>	Quality Committee 25 April 2018 Information Sub-Committee 12 April 2018		

<b>Key points</b>	<b>Purpose:</b>
1. There were no Level 2 High Risk reportable incidents in Quarter 4 of this past year.	To discuss and note
2. The Foundation Trust was fully compliant with IG training at 31 March 2018 at 96%. Training requirements will be changing for 2018/19.	To note and gain assurance
3. The Foundation Trust's IG Toolkit for 2018/19 was submitted on 29 March 2018 with a Level 2 'Satisfactory' status.	To discuss and note
4. Work continues with improvements aligned with changing data protection legislation (General Data Protection Regulation and UK law) and ongoing improvement work.	To note and gain assurance
5. The Board of Directors is asked to note the current position of Information Governance in the Foundation Trust.	To discuss and note

<b>Executive Summary:</b>
<p>It is a requirement of the Information Governance Toolkit (IGT) that the Senior Information Risk Owner (SIRO) regularly reports to the Board of Directors to identify information governance risks and action taken. This paper is the 2017/18 Quarter 4 update.</p> <p>There were no High Risk Level 2 reportable Information Governance incidents in this quarter. The Foundation Trust had a total of one High Risk Level 2 reportable information governance incidents for the financial year 2017/18. There were no cyber security incidents this period.</p> <p>Information governance mandatory training is fully compliant at year end with 95%.</p> <p>Current areas of focus are preparing for updates to data protection legislation (General Data Protection Regulation (GDPR) and UK law) as well as ongoing improvement work. This has included a strong focus on refreshing the Foundation Trust's Information Asset Management programme, contributing assurance in all these areas.</p> <p>The year end submission of the Information Governance Toolkit version for 2017-18 was submitted on 29 March 2018. With a Level 2 'Satisfactory' rating.</p> <p>The Board of Directors is asked to note the current position of Information Governance in the Foundation Trust.</p>

Board of Directors: 10.5.18

Agenda Item: Bo.5.18.11

<b>Financial implications:</b>	
No	
<b>Regulatory relevance: Data Protection Act 1998 (and incoming General Data Protection Regulation from May 2018)</b>	
<b>Monitor:</b>	Annual Reporting Manual Quality Governance Framework
<b>Equality Impact / Implications:</b>	<p><b>Is there likely to be any impact on any of the protected characteristics?</b>          (Age, Disability, Gender, Gender Reassignment, Pregnancy and Maternity, Race, Religion or Belief, Sexual Orientation, Health Inequalities, Human Rights)</p> <p>Yes   <input type="checkbox"/>                      No   <input checked="" type="checkbox"/></p> <p>If yes, what is the mitigation against this?</p>
<b>Other:</b>	Requirement to comply with relevant information rights related legislation and codes of practice, including but not limited to data protection legislation, the Common Law Duty of Confidentiality and various legislation relating specifically to digital records. Financial penalties of up to £500,000 for non-compliance. Updated data protection legislation (General Data Protection Regulation and supporting Data Protection Act, currently in House of Commons as a Bill) will allow fines of up to 2-4% of organisation turnover from 25 May 2018.
<b>Strategic Objective:</b>	To provide outstanding care for patients
<b>Reference to Strategic Objective(s) this paper relates to</b>	To be a continually learning organisation
	To collaborate effectively with local and regional partners

### Senior Information Risk Owner 2017/18 Quarter 4 Update

This is the 2017/18 Quarter 4 update from the Senior Information Risk Owner (SIRO).

#### 1. Information Governance Risk Incidents

During Quarter 4 the Foundation Trust received notification of 53 information governance-related risk incidents that have been reviewed and graded as shown below. The number of reported incidents in this quarter is similar to the number of incidents which were reported in the previous quarters.

**Board of Directors: 10.5.18**  
**Agenda Item: Bo.5.18.11**

Incident themes are reviewed and followed up. There are currently no particular 'hot spots' of teams or services.

There is one open incident with the Information Commissioner's Office (ICO) from December 2017.

**Table 1: Number of Incidents by rating**

Incidents	2016/17			2017/18											
	Q4			Q1			Q2			Q3			Q4		
	Jn	Fb	Mr	Ap	My	Jn	JI	Ag	Sp	Ot	Nv	Dc	Jn	Fb	Mr
SIRI High Risk Level 2 (reportable)	0	1	1	0	0	0	0	0	0	0	0	1	0	0	0
SIRI Level 1	9	9	21	10	15	15	18	13	8	7	6	2	5	4	2
SIRI Level 0 and below	7	4	11	6	7	3	5	3	5	7	14	13	15	13	14
No Trust involvement	0	2	3	1	1	2	2	1	0	0	0	0	0	0	0
Not rated	0	1	2	3	0	1	0	1	0	2	2	0	0	0	0

## 2. Information Security

Technical and organisational measures to ensure security of information are important parts of information governance. The Foundation Trust has continued to ensure that the systems and processes to identify, intercept and manage attacks are robust and raising staff awareness is ongoing. No electronic breaches have been reported this quarter.

The IG Sub-Committee continues to receive regular updates on the cyber security position and supporting Key Performance Indicators have been added to both the Informatics Performance and the Information Governance regular reports to support ongoing assurance.

An annual report was reviewed by the Sub-Committee noting additional controls and procedures put in place this year. No major concerns were raised in the report. The report included a plan for the coming year to make further improvements to security.

The Trust has been working towards an ISO27001 (International Information Security Standard) compliance. This will certify the Trust's email as secure with NHSMail.

**Board of Directors: 10.5.18**  
**Agenda Item: Bo.5.18.11**

---

### 3. Information Governance Mandatory Training

All staff members are required to complete mandatory IG training on an annual basis as a recognised measure to reduce the number of high risk IG incidents. A review of training compliance by division is presented below up to the end of March 2018. The IG Toolkit compliance requires 95% of staff to be in date with training. The Trust is compliant.

**Table 2: Training Levels by Divisions**

% Complete	2017/18											
	Ap	My	Jn	Jl	Au	Sp	Ot	Nv	Dc	Jn	Fb	Mr
Medicine & Integrated Care	78%	75%	73%	75%	81%	88%	90%	91%	91%	91%	92%	94%
Anaesthesia, Diag. and Surgery	74%	73%	71%	74%	79%	86%	89%	89%	89%	89%	90%	97%
Women & Children	75%	72%	73%	74%	80%	89%	89%	88%	88%	88%	95%	97%
Core Central Services	83%	80%	83%	81%	81%	84%	86%	87%	86%	86%	90%	94%

There continues to be a variety of methods and mechanisms to complete training. From 2018/19, the training plan will be updated to include the nationally mandated Data Security and Protection online training, which will be essential to compliance with the updated Toolkit.

The IG Team continues to respond to queries, support regular training sessions, advise staff, and complete ward 'spot checks' to review key actions including signage, secure use of IT, management of live records, disposal of confidential waste, use of identification/Smartcards, and to discuss any concerns that staff may have.

### 4. Information Governance Toolkit 2017/18 and Data Security & Protection Toolkit 2018/19

The Information Governance Toolkit (IGT) is a self-assessment tool managed and hosted by NHS Digital on behalf of the Department of Health. The IGT is a compilation of evidence that provides assurance that the Foundation Trust is compliant with IG legislation and best practice, Department of Health directives and other national guidance. The final submission of the IGT was made on 29 March 2018, with a status of Level 2 'Satisfactory'. There are only two possible outcomes: Satisfactory or Unsatisfactory.

From 2018/19 the IG Toolkit is converting into the national Data Security & Protection Toolkit, which is a prototype at present. The new Toolkit has ten standards based on the National Data Guardian's 2016 Review of Data Security, Consent and Opt Outs<sup>1</sup>. The new Toolkit has greater focus on information and cyber security assurance and staff awareness. Work is underway to ensure compliance.

**Board of Directors: 10.5.18**  
**Agenda Item: Bo.5.18.11**

---

## **5. Information Governance Audits**

There has been a number of Internal Audit review related to information governance, as follows:

- The regular annual audit of a sample of the IG Toolkit pre-submission with an outcome of Significant Assurance.
- Audit of status submitted for actions on Information Commissioner's Office (ICO) Best Practice Review recommendations with an outcome of Significant Assurance.
- Review of the Trust's readiness at that point in time for changes to data protection legislation (General Data Protection Regulation) with an outcome of Significant Assurance noting completion of the work is needed.

## **6. Data Quality**

The Trust continues to improve upon the quality of the data used within the organisation via reporting tools including EPR, Data warehouse and the Dashboard to monitor data quality including trends and operational impact. An operational data quality group continues and a four person team of operational managers and business intelligence staff have been seconded to both expedite and bed-in this work.

## **7. Freedom of Information**

The Freedom of Information team has handled over 600 requests during 2017-18. The team processed 95% of requests within the statutory period of 20 working days.

## **8. Subject Access Requests**

The Access to Medical Records Team continue to receive regular requests. The team processed 100% requests within the statutory period of 40 working days.

## **9. ICO Best Practice Review**

The status and supporting evidence for the actions associated with the ICO Best Practice review were sent to the ICO in December 2017 as agreed. The status was reviewed by a different team from the one that undertook the initial site visit which contributed to there being a number of followup questions. Further evidence was submitted in January 2018. The ICO has noted progress in all areas with recognition that there is ongoing work to implement compliance with new data protection legislation and embed internal processes around privacy impact assessments and information security. The work with the ICO on the Best Practice Audit is now closed with the ICO. The Trust continues to make improvements towards best practice.

## **10. General Data Protection Regulation**

The General Data Protection Regulation (GDPR) will be in force from 25 May 2018 and data protection legislation is currently in the House of Commons at Bill stage to implement GDPR into UK law and replace the current Data Protection Act (1998). National guidance that was anticipated from NHS England and NHS Digital has been limited and NHS organisations were informed during the third quarter of 2017-18 that there would be no national framework to support the processes common to all.

**Board of Directors: 10.5.18**

**Agenda Item: Bo.5.18.11**

---

A working group has been set up for BTHFT to focus on ensuring that remaining is completed with members drawn from the key impacted areas - Human Resources, Business Intelligence, Patient Experience and Subject Access Requests.

The key areas continue to be:

- Contracts and agreements
- Communication and involvement with patients and public
- Subject access requests.

#### **11. Recent Information Commissioner's Office Enforcement Action**

There has been no ICO enforcement action against NHS organisations in Q4.

The ICO has pursued an increasing number of criminal prosecutions of private individuals for inappropriate access or use of personal data in relation to their employed role. The Electronic Patient Records training for staff includes reinforcement that access to patient records can be monitored/audited and must only be accessed or shared for provision of direct care to the patient (including commissioning reporting for payment) or when duly authorised by research, audit or other Trust approved process for use of data for planning or service improvement purposes.

#### **12. Conclusion**

The Quality Committee is asked to note the current position of information risk in the Foundation Trust