

<b>Report to:</b>	Board of Directors				
<b>Date of Meeting:</b>	29 <sup>th</sup> April 2015				
<b>Report Title:</b>	Information Governance Annual Report 2014/15				
<b>Status:</b>	<b>For information</b>	<b>Discussion</b>	<b>Assurance</b>	<b>Approval</b>	<b>Regulatory requirement</b>
Mark relevant box with X	x		x		
<b>Prepared by:</b>	Tim Rycroft, Head of Information Technology & Information Governance Juliet Norris, Information Governance Officer				
<b>Executive Sponsor (presenting):</b>	Andrew Copley, Director of Finance				
<b>Appendices (list if applicable):</b>	Appendix 1: Information Governance Annual Report 2014/15				

<b>Purpose of the Report</b>
<p>The purpose of this report is to:</p> <ol style="list-style-type: none"> <li>1. Update the Board of Directors on the Information Governance (IG) programme, confirming the results of the Toolkit assessment for 2014/15 and internal audit outcome.</li> <li>2. Provide an overview of the arrangements in place to manage information risks and improve compliance in the year ahead.</li> </ol>
<b>Key points for information</b>
<ol style="list-style-type: none"> <li>1. <b>Toolkit.</b> The Trust achieved an overall score of '<b>Satisfactory</b>' with 38 criteria at the minimum level 2 and 6 criteria exceeding the minimum at level 3.</li> <li>2. <b>Audit.</b> MIAA audited a sample of 12 requirements alongside spot-checks within a cross-section of Trust services. Their overall opinion was '<b>Significant</b>' assurance.</li> <li>3. <b>FOI.</b> The Trust received 500 FOI requests between 01/4/2014 – 31/03/2015, almost exactly the same as last year. There have been no complaints made by requesters to date.</li> <li>4. <b>Access to Health Records.</b> During 2014/15, the Trust received 1065 requests for Access to Health Records, an average of 88.5 per month. There were 21 breaches of the 40 day response time; often due to notes not being available. The service ensures that customers are made aware of any potential delays. The department is not aware of any complaints being received in relation to the service.</li> <li>5. <b>Information Governance Incidents.</b> The Trust reported one Serious Information Governance Reportable Incident during 2014/15. The incident involved the disclosure of one patient's clinical data, in error, to a third party. The incident was logged and managed via the Trust internal process.</li> </ol>

6. **New powers given to the ICO:** From 1 February, the ICO will be able to subject public healthcare organisations to a compulsory audit. These compulsory audits have previously only applied to central government departments. The Information Commissioner has welcomed a change in the law that will give his office the right to force NHS authorities to be audited for compliance with the Data Protection Act.
7. **Final Summary.** The Trust has a robust process for managing IG and the associated responsibilities that come with our commitment to adopt best practice processes and procedures in order to protect patient and service users' information. It has a dynamic action plan to refresh and improve its compliance with the Toolkit standards.

---

**Recommendation**

---

The Board of Directors are asked to receive and note this report.

## INFORMATION GOVERNANCE ANNUAL REPORT 2014/15

### 1) PURPOSE

Further to reports to EAG in February and March 2015, the purpose of this report is to;

- update the Board on the Information Governance (IG) programme, confirming the results of the Toolkit assessment for 2014/15 and internal audit outcome, and
- provide an overview of the arrangements in place to manage information risks and improve compliance in the year ahead.

### 2) IG TOOLKIT ASSESSMENT 2014/15

The IG Toolkit is a tool produced by the Department of Health and draws together the relevant information management legislation, national and international guidance under a single framework designed to enable an organisation to implement the relevant standards. It enables the Trust to measure its performance through an annual self-assessment audit process and report upon levels of compliance against a set number of requirements. There are a number of levels:

NR	Not relevant
0	No or insufficient evidence, not satisfactory for compliance
1	Limited evidence, not satisfactory for compliance
2	Minimum level satisfactory for compliance
3	Evidence of further processes, measures & controls, satisfactory for compliance

The Trust is required to measure itself against 45 requirements. These are broken down into the above levels and then each level contains several questions. Every answer at each level requires supporting evidence. In total this requires several hundred individual items of evidence,

Organisations can only achieve a final overall score of “Satisfactory” by scoring a minimum Level 2 for **all** requirements. This is regardless of the amount of progress made against individual requirements. The submission for 2014/15 took place on 26<sup>th</sup> March 2014. The Trust achieved an overall score of ‘Satisfactory’ with 38 criteria at the minimum level 2 and 6 criteria exceeding the minimum at level 3.

Prior to submitting its final assessment, the Trust’s internal auditors, MIAA audited a sample of 12 requirements alongside spot-checks within a cross-section of Trust services. **Their overall opinion was ‘Significant’ assurance.** The Board can take assurance that the controls upon which the organisation relies to manage IG are suitably designed, consistently applied and effective. See Appendix B assessment summary.

### 3) COMPLIANCE WITH LEGAL AND REGULATORY FRAMEWORK

Compliance with key legislation, such as the Data Protection Act 1998 (DPA) and Freedom of Information Act 2000 (FOIA) is regulated by the Information Commissioner’s Office (ICO). Internally, the IG Group monitors compliance with the FOIA and DPA.

The Trust received 500 FOI requests between 01/4/2014 – 31/03/2015, almost exactly the same as last year. It should be noted that the volume of requests can really give no

indication of the amount of time spent in answering each one. Some requests involve reporting on data that we routinely collect and can be completed relatively quickly, but others may involve large amounts of work by different departments and we frequently have to judge whether answering a request would exceed the 18 hours “appropriate cost limit”.

There have been no complaints made by requesters to date, although requests continue to rise, a situation reflected across the entire NHS. Unfortunately, we are also increasingly receiving requests from staff at other NHS Trusts and organisations using the Act as a quicker way of attaining information. FOIA remains a challenge to manage and for different areas of the business to respond to.

Future plans: The IG Service would like to publish completed requests on the Trust’s public facing website. This would demonstrate best practice as detailed in the ICO’s model publication scheme and contribute to building a knowledge library of data which external applicants can access. This process may help reduce the number of requests received by the Trust, given that many requests relate to commonly themed topics. During 2015/15 the IG Service will look at how this improvement can be achieved.

### **Access to Health Records**

During 2014/15, the Trust received 1065 requests for Access to Health Records, an average of 88.5 per month. Requests come from patients themselves, their representatives, third parties and other agencies such as social services, the police and continuing care (local authorities). There were 21 breaches of the 40 day response time; often due to notes not being available. The service ensures that customers are made aware of any potential delays. The department is not aware of any complaints being received in relation to the service.

## **4) INFORMATION GOVERNANCE INCIDENTS**

The Trust reported one Serious Information Governance Reportable Incident during 2014/15. The incident involved the disclosure of one patient’s clinical data, in error, to a third party. The disclosed data was recovered by the Trust. The incident was logged and managed via the Trust internal process. In addition it was graded at level 2 in accordance with the national IG Serious Incident Requiring Investigation (SIRI) tool and reported externally to the Information Commissioner’s Office (ICO) and Department of Health.

## **5) RISK MANAGEMENT AND ASSURANCE**

The Senior Information Risk Owner (SIRO) is responsible for overseeing the development and implementation of the information risk strategy. The SIRO is supported in this by the Information Governance team and by Information Asset Owners (IAO). The IAO is responsible for managing information risks to the assets within their control. This involves developing system security policies (SLSP) and business continuity plans as well as documenting their personal data information flows and conducting regular information risk assessments.

The Head of IT and IG and Trust’s information security lead support IAOs in achieving these objectives. Whilst progress has been made again during 2014/15, further work is required to embed these processes further.

The Toolkit is a standing agenda item for the IG Group. Requirement owners must alert the Group to any high risks, that is where the completion of certain actions are critical to achievement of Level 2, and where there are significant concerns that actions may not be

completed. These are managed through a local risk register, are highlighted to the SIRO, included in any reporting, and escalated if appropriate.

## 6) IMPROVEMENT PLAN

Appendix A is an extract from the draft improvement plan showing Toolkit actions carried forward from 2014/15. New actions have also been included based on the outcome of the assessment and recommendations from the internal audit review. The plan itself is a more comprehensive “live” document forming part of the online Toolkit. It enables a requirement owner, in agreement with IG, to set and manage all actions. Actions are reviewed, progressed and monitored by the IG Group. The plan is developed and updated throughout the year.

## 7) SUMMARY

The Trust has a robust process for managing IG and the associated responsibilities that come with our commitment to adopt best practice processes and procedures in order to protect patient and service users’ information. It has a dynamic action plan to refresh and improve its compliance with the Toolkit standards.

Evidence for many of the requirements is refreshed as part of established daily business or monitoring activities. However, some objectives are more challenging and for this reason are being targeted already. Key areas are to:

- Promote and monitor the uptake of IG training
- Continue embedding Information Governance best practice within the culture of the organisation, through additional awareness and training
- Work with the Caldicott and Risk department to target IG incident ‘near misses’ with a view to reducing the potential for IG SIRIs
- Work with IAOs to embed effective information risk management activities
- Review and update the annual information workflow exercise to capture new flows, and ensure that data sharing agreements and/or appropriate IG controls are in place
- Review the Trust contracts register to ensure key contracts are aware of updated IG clauses.
- Support the Trust’s strategy and management of data quality

We must continue to respond to the challenges faced by changing working practices in order to ensure that we keep pace with the ever-changing information society we work in. Going forward, this will only become even more demanding. National developments will have a bearing on the direction of the Information Governance programme.

- **Caldicott2 IG review recommendations:** still being implemented nationally
- **New powers given to the ICO:**

From 1 February, the ICO will be able to subject public healthcare organisations to a compulsory audit. These compulsory audits have previously only applied to central government departments.

The Information Commissioner has welcomed a change in the law that will give his office the right to force NHS authorities to be audited for compliance with the Data Protection Act.

The audits review how the NHS handles patients' personal information, and can review areas including security of data, records management, staff training and data sharing.

The ICO will be able to assess data protection by England's NHS foundation trusts, GP surgeries, NHS Trusts and Community Healthcare Councils, and their equivalent bodies in Scotland, Wales and Northern Ireland under section 41A of the Data Protection Act.

To date, the ICO has issued fines totalling £1.3m to NHS organisations.

- **The new EU DPA regulation:** pending

We will continue to work with other NHS organisations in our region sharing good practice, and to aim for an integrated approach.

The IG Group asks the Board to receive and note this report. It is asked to support plans to ensure that the Trust achieves an overall satisfactory position by achieving a minimum Level 2 for all requirements for 2015/16 and crucially, that it continues to improve and embed IG into routine working practice across the Trust.

**13 April 2015**

Tim Rycroft, Head of IG and IT  
Juliet Norris, IG Officer

**Appendix A: Extract from IG Over-Arching Work Plan 2015/16**

IGT req.	Action	Action owner	Deadline	Progress	Status
<b>Over-Arching Objectives</b>					
Supports whole Toolkit	Review IG Framework / Strategy and associated policies in line with latest guidance. Streamline publication and control of each.	T Rycroft / J Norris	30/09/2015	Pending	open
Supports whole Toolkit	Review IG Guidance for Staff and Public: includes methods of publication. Include emphasis on Trust Code of Confidentiality.	T Rycroft / J Norris	31/12/2015	Pending	open
Supports whole Toolkit	Review IG Training Materials / Methods of Delivery	T Rycroft / J Norris / with Workforce Development	31/12/2015	Pending	open
Supports whole Toolkit	Review of Trust Information Asset Register and supporting SLSP process.	T Rycroft / J Norris / IT Systems Manager	31/01/2016	Pending	open
Supports whole Toolkit	Monitor provision of fair processing posters (privacy notices)	T Rycroft / J Norris	31/03/2016	On-going throughout the year	open
Supports whole Toolkit	Review IG Sharepoint / Intranet Presence	T Rycroft / J Norris	31/03/2016	On-going throughout the year	open
Supports whole Toolkit	Work with the Caldicott and Risk department to target IG incident 'near misses' with a view to reducing the potential for IG SIRIs	T Rycroft / J Norris	31/03/2015	On-going throughout the year	open
<b>Criteria Specific Objectives</b>					

110	Review the Trust contracts register to ensure key contracts are aware of updated IG clauses	Tim Rycroft	31/03/2016	instructions issued in part for key system	open
112 (2a)	Audit Recommendation is for the Trust to achieve 95% staff compliance with IG Mandatory training, as per the national mandate.	T Rycroft / J Norris	31/03/2016	Pending	open
207 (2b)	Review Information Sharing Protocols	IG Group	31/03/2016		open
210 (2b)	Strengthen PID/PIA documentation for new projects	T Rycroft / J Norris	31/12/2015		open
300 (2b)	All staff assigned responsibility for Information Security have been appropriately trained to carry out their role.	T Rycroft / J Norris	31/12/2015		open
323 (level 2)	Review Level 2 based on Audit comments: “The provision of all mandatory and additional safeguards is only partially covered by submitted evidence, or is not explicit enough. This primarily relates to the provision of centralised controls that would normally be provided by IT. It is accepted the controls probably exist but the supporting framework needs some enhancement”.	T Rycroft / J Norris	31/12/2015		open
505 (level 2)	Review Level 2 based on Audit comments: “IG in year audit providing required coverage and key statistics not available at time of review. It is acknowledged this was scheduled and previous years provides confidence in overall process. It is also suggested that management consider bringing this process forward in the year in advance of winter pressures to simplify sign off of this requirement.”	T Rycroft / J Norris with I Hargreaves	31/03/2016		open