Surrey and Sussex NHS
Healthcare NHS Trust

TRUST BOARD IN PUBLIC		Date: 29 June 2017 Agenda Item: 6.2
REPORT TITLE:		Information Governance Annual report
EXECUTIVE SPONSOR:		Ian Mackenzie
REPORT AUTHOR:		Dipa Bhella
REPORT DISCUSSED PREVIOUSLY: (name of sub-committee/group & date)		IGSG members: June 2017
Action Required:		
Approval ( )	**Discussion ( )**	**Assurance (√)**

Purpose of Report:

The purpose of this report is to provide assurance to the Board that the Trust is addressing information governance (IG) obligations.

Summary of Key Issues

The Trust is in its fifth year of achieving 'satisfactory' rating in the Information Governance Toolkit assessment.

To achieve an overall organisational rating of 'satisfactory' (the highest level possible), all 45 requirements must be scored at level 2 or above.

This report can be summarised as containing:

- IG Toolkit Assessment 2016/17
- Assurance Framework
- Compliance with Legal and Regulatory Framework
- Information Security Incidents
- Risk Management and Assurance
- Development Plans for Next Year

Recommendation

The Board is asked to note the report.

Relationship to Trust Strategic Objectives & Assurance Framework:

SO1: Safe -Deliver safe, high quality care **and improving** services which pursue perfection and be in the top **25% of** our peers
SO2: Effective – As a teaching hospital, deliver effective and improving sustainable clinical services within the local health economy
SO3: Caring – Work **with compassion** in partnership with patients, staff, families, carers **and community partners**
SO4: Responsive To **continue to be** the secondary care provider of choice for the **people of our community**
SO5: Well led – To be a **high quality** employer of choice and deliver financial and clinical sustainability around a patient centred, clinical led leadership model.

Corporate Impact Assessment:	
Legal and regulatory implications	Ensures the Board is aware of the Trust's compliance with key legislation and broader information governance compliance
Financial implications	N/A
Patient Experience/Engagement	N/A
Risk & Performance Management	Informs the Board of the Information Governance Risk and Assurance Framework
NHS Constitution/Equality & Diversity/Communication	N/A
Attachments:	

TRUST BOARD REPORT – 29 June 2017

Information Governance (IG) Annual Report to the Board

1. Introduction

1.1. The purpose of this report is to provide assurance to the Board that the Trust is addressing information governance (IG) obligations.

This report comments on:

1.1.1. compliance with the Information Governance toolkit and improvements in relation to managing risks to information

1.1.2. organisational compliance with legislative and regulatory requirements relating to the handling of information, including compliance with the Data Protection Act (1998) and Freedom of Information Act (2000);

1.1.3. any Serious Untoward Incidents within the preceding twelve months, relating to any losses of personal data or breaches of confidentiality.

1.1.4. the direction of information governance work during 2016/17 and how it aligns with the strategic objectives of Surrey and Sussex Healthcare NHS Trust.

2. Information Governance Toolkit Assessment

2.1. The Information Governance Toolkit is the mechanism through which NHS and related organisations demonstrate their compliance with a number of information governance requirements – of which there are 45 for the acute hospital sector.

2.2. The Trust is required to upload evidence to support its assessment of its compliance against criteria set within the toolkit. This then determines the scores for each requirement which range from level zero to three. To achieve an overall organisational rating of 'Satisfactory' (the highest level possible), each requirement must be scored at level 2 or above.

2.3. Caldicott 2 Performance Report – From August 2015 Trusts are required to submit an annual report demonstrating their performance against the Caldicott2 recommendations. To show that a trust has fully implemented a particular Caldicott 2 recommendation, they will need to demonstrate all relevant IG Toolkit requirements within a recommendation are attaining level 3. Eight out of nine Caldicott 2 recommendations have been fully implemented.

2.4. Prior to submitting its final assessment, the Trust's internal auditors, RSM Tenon, audited a random sample of 11 requirements based on the interim scores submitted by the Trust in October 2016. Based on the evidence available at the time of the audit, they agreed the scores of eight of the requirements. For the three unsubstantiated items the Trust simply had not updated the full evidence for these items as yet in 2016/17. In order to satisfy the requirements of the submitted scores additional evidence was uploaded before final submission.

2.4.1 The audit report concluded the Trust's procedures for managing IG Toolkit improvement plans, including monitoring, reporting, and compliance with the three-stage reporting timescale set by NHS Digital, were found to be robust, and thus reduce the risk of failure or delay in implementing improvements to the Trust's submissions and achievement of target levels regarding Toolkit compliance.

2.5. In the year ending 31st March 2017, the Trust achieved an overall rating of 'Satisfactory'. The breakdown of the scores are shown in the table below:

Table 1: SASH IG Toolkit Final Assessment (2016/2017)

Assessment	Level 0	Level 1	Level 2	Level 3	Total Req'ts	Overall Score	Grade
Information Governance Management	0	0	2	3	5	86%	Satisfactory
Confidentiality and Data Protection Assurance	0	0	4	5	9	85%	Satisfactory
Information Security Assurance	0	0	11	4	15	75%	Satisfactory
Clinical Information Assurance	0	0	4	1	5	73%	Satisfactory
Secondary Use Assurance	0	0	5	3	8	79%	Satisfactory
Corporate Information Assurance	0	0	2	1	3	77%	Satisfactory
Overall	**0**	**0**	**28**	**17**	**45**	**79%**	**Satisfactory**

2.6. The Trusts results are comparable with other Acute Trusts within Surrey and Sussex as shown below:

Table 2: Overall IG Toolkit Scores: Acute Hospitals in Surrey & Sussex

Assessment	Level 0	Level 1	Level 2	Level 3	N/R *	Total Req'ts	Overall Score	Grade
ASPH	0	0	38	7	0	45	71%	Satisfactory
BSUH	0	0	43	1	1	45	66%	Satisfactory
East Sussex	0	0	39	6	0	45	71%	Satisfactory
Frimley Health	0	0	32	13	0	45	76%	Satisfactory
RSCH	0	0	41	4	0	45	69%	Satisfactory
SASH	0	0	28	17	0	45	79%	Satisfactory
Western Sussex	0	0	28	17	0	45	79%	Satisfactory

2.7. Information Governance Training: with the recent guidance issued by NHS Digital in December 2016 and the decommissioning of the online tool the trust continued to train staff via face to face sessions and workbooks and focused on training new starters.

2.8. The revised online training tool will include material on cyber security and covers aspects of social engineering, email phishing and malware; a date is yet to be confirmed. As of April 2017 the IG team has launched the interim workbooks published by NHS Digital to ensure all staff receives training on the new material as soon as possible.

3. Assurance framework

3.1. The Trust's Information Governance Management Framework was reviewed in June 2016. It identifies the roles and responsibilities of key staff within the Trust and the reporting structures.

3.2. The Information Governance Steering Group (IGSG) is chaired by the Trust's Senior Information Risk Owner (SIRO), who is the Director of Information and Facilities. Membership includes the Caldicott Guardian (the Medical Director) and representatives from Human Resources, Finance, Information Technology, Information Management and Data Quality, Health Records, Communications and Information Governance.

3.3. The reporting framework is as follows:

4. Trust Compliance with Legal and Regulatory Framework

4.1. 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 IGSG monitors compliance with the FOIA and DPA at each of its meetings.

4.2. **Freedom of Information Requests**: The Trust received 667 FOI requests during 2016/17. There were 127 breaches of the FOI 20 working day response standard in the year to date.

4.3. Compared to previous year the Trust's overall compliance has dropped from 90% to 81%. These have largely been due to delays in staff supplying information and the increase in the number of FOI requests received.

4.4. **Table 3: FOIA Compliance**

2016/2017	**Q1**	**Q2**	**Q3**	**Q4**	**Grand Total**
Received	162	169	152	184	667
Compliant	141	126	117	154	538
Breach	21	43	35	30	122
% Compliance	**87.6**	**74.5**	**76.9**	**83.6**	**80.6**

4.5. **Subject Access Requests:** In the year 2016/17 the Trust received 1103 enquiries relating to accessing health records (92 monthly average).

4.6. **Table 4: SAR Compliance**

2016/2017	Q1	Q2	Q3	Q4	Grand Total
Received	294	245	268	296	1103
Compliant	294	245	268	296	1103
Breach	0	0	0	0	0
% Compliance	**100%**	**100%**	**100%**	**100%**	**100%**

Since April 2016 the SAR's team have focused on reducing the amount of time to process a SAR's request. 99% of all requests were processed within 21 days.

The Trust did receive one complaint via the regulator, the Information Commissioner, over the Trust's handling of subject access requests. The complaint related to the patient's request for access to their health records. The complaints has been closed which demonstrated the request had been dealt with appropriately.

5. Information Security Incidents

5.1. Staff are encouraged to report information governance risks and incidents. All incidents were classified as either level zero or level one in accordance with DH guidance[1]. Incidents greater than level 2 are reportable to the Information Commissioners Office. As table 4 below shows the majority of incidents reported, relate to patient records; these incidents include failure to secure records, records found in a public place and disclosed in error.

Outcomes of incidents and lessons learnt are reported to staff at training awareness sessions.

1

Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation: Version 5.1_May 2015

5.2. **Table 4: Information Security Incidents**

2016/17	Q1	Q2	Q3	Q4	Total
Email	2	1	4	1	8
Patient records confidentiality	17	23	22	23	85
Post	3	1	2	3	9
Printer / Fax	1	0	0	1	2
Smartcards / Passwords	1	0	2	1	4
Staff records	1	0	0	1	2
Verbal breach	0	0	0	0	0
Other	0	1	1	0	2
Total	**25**	**26**	**31**	**30**	**112**

6. Risk Management & Assurance

6.1. As well as line management responsibility for information governance manager, the SIRO is responsible for overseeing the development and implementation of the Trust's information risk strategy.

6.2. The SIRO is supported in this by the Information Governance Manager and by Information Asset Owners (IAOs) within each business area. The IAOs are responsible for managing information risks to the assets within their control. This involves developing system security policies and business continuity plans as well as documenting their personal data information flows, updating asset registers, conducting regular information risk assessments, and ensuring staff have completed their annual information governance training.

6.3. The IAOs reviewed the system security policies and risk assessments for their information assets. Overall no information assets have been highlighted as 'red risks', and show that robust controls are in place to reduce the impact of risks that may occur.

6.4. Whilst progress was made, the Trust recognises that further work is required to embed further assets to these processed.

7. Development plans for next year

7.1. The Trust has a dynamic action plan to refresh and improve its compliance with the IG Toolkit standards. This will be formally reviewed once the toolkit is published for the year ahead.

7.2. Evidence for many of the toolkit requirements is readily refreshed as part of established daily business or monitoring activities. However, some objectives are harder to achieve and for this reason they are being targeted early on.

7.3. Key areas identified for 2017/18 are to:

7.3.1. Review evidence and maintain the scores of the IG toolkit at level 2 and above

7.3.2. Identify the evidence required to achieve level 3 on the requirements

7.3.3. Promote and monitor the uptake of data security awareness training which requires 95% of staff to undertake or refresh their training annually. In recent light of the NHS Cyber-attack staff will be instructed to complete training by end of September 2017

7.3.4. Maintain compliance with Subject Access Requests and improve compliance with Freedom of Information requests.

7.3.5. Review and map data flows in each area

7.3.6. Prepare for the General Data Protection Regulation (GDPR) to be implemented by May 2018.

8. Summary and recommendations

8.1. In summary, much has been achieved in the last year, which is supported by the 'Satisfactory' rating in the IG Toolkit assessment and internal audit opinion.

8.2. The executive committee is asked to receive and note this report.

Ian Mackenzie
Director of Information & Facilities
June 2017