Surrey and Sussex NHS
Healthcare NHS Trust

TRUST BOARD IN PUBLIC		Date: 30th June 2016 Agenda Item:
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: 27th May 2016
Action Required:		
Approval ( )	**Discussion ( )**	**Assurance (√)**

Summary of Key Issues

The Trust is in its fourth 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.

- IG Toolkit Assessment 2015/16
- Assurance Framework
- Compliance with Legal and Regulatory Framework
- Information Security Incidents
- Risk Management and Assurance
- Development Plans for Next Year

Relationship to Trust Strategic Objectives & Assurance Framework:

SO1: Safe -Deliver safe services and be in the top 20% against our peers
SO2: Effective - Deliver effective and sustainable clinical services within the local health economy
SO3: Caring – Ensure patients are cared for and feel cared about
SO4: Responsive – Become the secondary care provider and employer of choice for the catchment populations of Surrey & Sussex
SO5: Well - led

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 – Date June 2016

Information Governance Annual Report to the Board – Senior Information Risk Owner

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 2015/16 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 now 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.

2.4. Prior to submitting its final assessment, the Trust's internal auditors, RSM UK, audited the requirements against the Caldicott 2 recommendations. Based on the evidence available at the time of the audit, agreed the scores of all eleven of the requirements. 10 out of 11 Caldicott 2 recommendations have been fully implemented.

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 HSCIC, 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 2016, 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 (2015/2016)

Assessment	Level 0	Level 1	Level 2	Level 3	Total Req'ts	Overall Score	Grade
Information Governance Management	0	0	4	1	5	73%	Satisfactory
Confidentiality and Data Protection Assurance	0	0	4	5	9	85%	Satisfactory
Information Security Assurance	0	0	12	3	15	73%	Satisfactory
Clinical Information Assurance	0	0	3	2	5	80%	Satisfactory
Secondary Use Assurance	0	0	6	2	8	75%	Satisfactory
Corporate Information Assurance	0	0	2	1	3	77%	Satisfactory
Overall	**0**	**0**	**31**	**14**	**45**	**77%**	**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	Total Req'ts	Overall Score	Grade
ASPH	0	1	21	23	45	85%	Not Satisfactory
BSUH	0	0	44	0	45	66%	Satisfactory
East Sussex	0	0	39	6	45	71%	Satisfactory
Frimley Health	0	5	27	13	45	72%	Not Satisfactory
RSCH	0	0	40	5	45	70%	Satisfactory
SASH	0	0	31	14	45	77%	Satisfactory
Western Sussex	0	0	21	24	45	84%	Satisfactory

2.7.1. Ashford and St Peter's Hospital and Frimley Health were deemed 'not satisfactory' because they have requirements at level 1.

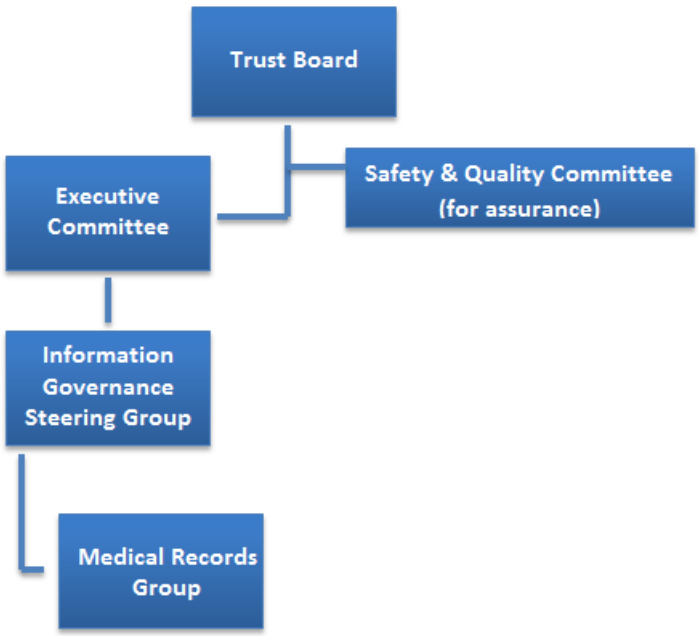
2.7. Information Governance Training: 96% of staff completed their annual information governance training during 2015/2016 this now needs to be refreshed for 2016/17. 95% of staff must complete their training each financial year, for the Trust to achieve level 2 in this requirement of the IG Toolkit assessment.

3. Assurance framework

3.1. The Trust's Information Governance Management Framework was reviewed in June 2015. 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 561 FOI requests during 2015/16. There were 56 breaches of the FOI 20 working day response standard in the year to date. These have largely been due to delays in staff supplying information.

4.3. Compared to previous year the Trust has maintained its compliance, achieving an overall compliance rate of 90%.

4.4. **Table 3: FOIA Compliance**

2015/2016	Q1	Q2	Q3	Q4	Grand Total
Received	125	169	116	151	561
Compliant	115	144	109	137	505
Breach	10	25	7	14	56
% Compliance	**92%**	**85%**	**94%**	**91%**	**90%**

4.5. **Subject Access Requests:** In the year 2015/16 the Trust received 1207 enquiries relating to accessing health records (101 monthly average).

4.6. **Table 4: SAR Compliance**

2015/2016	Q1	Q2	Q3	Q4	Grand Total
Received	348	324	254	281	1207
Compliant	287	322	254	284	1144
Breach	61	2	0	0	63
% Compliance	**82%**	**99%**	**100%**	**100%**	**95%**

There have been a small number of SAR breaches in quarter one mainly due to the complex process for reporting SAR's alongside staff shortage.

Since July 2015, an improved process for SAR's reporting has helped maintain compliance, improved governance arrangements; enabled potential issues to be identified earlier; and improved visibility and performance monitoring.

The Trust did receive two complaints 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. Both complaints have now 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.

The introduction of the new radio frequency identification tagging system that has been applied to the medical records has shown a reduction in incidents reported compared to previous year figures.

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

2015/16	Q1	Q2	Q3	Q4	Total
Email	0	3	1	0	4
Patient records confidentiality	13	24	24	20	**81**
Post	4	5	6	5	**20**
Printer / Fax	2	1	4	3	**10**
Smartcards / Passwords	1	0	2	0	**3**
Staff records	0	1	1	0	**2**
Verbal breach	2	1	1	1	**5**
Other	1	1	1	0	**3**
Total	**23**	**36**	**40**	**29**	**128**

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

[1] Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents Requiring Investigation: Version 5.1_May 2015

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. During 2015/2016 all IAO's completed their annual training in Information Risk Management via the e-learning tool.

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

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 2016/17 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 IG training which requires 95% of staff to undertake or refresh their training annually

7.3.3.1. Identify IG champions in key areas to promote training and increase compliance.

7.3.3.2. Promote IG refresher packs to clinical and non-clinical areas

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

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 Board is asked to receive and note this report.

Ian Mackenzie
Director of Information & Facilities
May 2016