Surrey and Sussex NHS Healthcare NHS Trust

TRUST BOARD IN PUBLIC	Date: 30th May 2013 Agenda Item: 5.5
REPORT TITLE:	Information Governance Annual Report
EXECUTIVE SPONSOR:	Ian Mackenzie Director of Information and Estates
REPORT AUTHOR:	Sarah Azhashemi Information Governance Manager
REPORT DISCUSSED PREVIOUSLY: (name of sub-committee/group & date)	Information Governance Steering Group Members: 16/05/2013

Purpose of the Report and Action Required:		**(√)**
This report provides members with the results of the 2012/13 IG Toolkit assessment and an overview of the arrangements in place to manage information risks and improve compliance in the year ahead.	**Approval**	
	Discussion	
	Information/Assurance	√

Summary: (Key Issues)

- IG Toolkit Assessment 2012/13
- Assurance Framework
- Compliance with Legal and Regulatory Framework
- Information Security Incidents
- Risk Management and Assurance
- Development Plans for Next Year

Relationship to Trust Corporate Objectives & Assurance Framework:

Central to all objectives and the assurance framework.

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:

None

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

1. Purpose

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

1.2. This report comments on:

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

1.2.2. 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);

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

1.2.4. the direction of information governance work during 2013/14 and how it aligns with the strategic business goals 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', each requirement must be scored at level 2 or above.

2.3. Prior to submitting its final assessment, the Trust's internal auditors, RSM Tenon, audited a random sample of 10 requirements and agreed the proposed scores, subject to one recommendation, which was completed before the submission. Their overall opinion was "Taking account of the issues identified, the Board can take substantial assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective".

2.4. In the year ending 31st March 2013, the Trust achieved an overall rating of 'Satisfactory'. The breakdown of the scores are shown in the table overleaf:

Table 1: SASH IG Toolkit Final Assessment (2012/2013)

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	8	1	9	70%	Satisfactory
Information Security Assurance	0	0	12	3	15	73%	Satisfactory
Clinical Information Assurance	0	0	5	0	5	66%	Satisfactory
Secondary Use Assurance	0	0	6	2	8	75%	Satisfactory
Corporate Information Assurance	0	0	3	0	3	66%	Satisfactory
Overall	**0**	**0**	**36**	**9**	**45**	**73%**	**Satisfactory**

2.5. 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		45	71%	Satisfactory
BSUH	0	0	44	0	1	45	66%	Satisfactory
E. Sussex Healthcare	0	0	41	4		45	69%	Satisfactory
FPH	0	0	32	13		45	76%	Satisfactory
RSCH	0	0	26	18	1	45	80%	Satisfactory
SASH	0	0	36	9		45	73%	Satisfactory
Western Sussex Hospitals	0	0	38	7		45	71%	Satisfactory

*Not relevant

3. Assurance framework

3.1. The Trust's Information Governance Management Framework was reviewed in July 2013. 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 Chief Medical Officer) 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**: during 2012/13 the Trust received 322 requests for information, an average of 27 per month. 84% of requests received a response within the 20 working day response time. There was a sharp increase in the number of breaches that occurred in the final quarter of the year. This was largely due to a number of staff changes that occurred during that period and the consequent learning curve, coupled with a peak of 36 requests received in January 2013.

4.3. Table 3: FOIA Compliance

2012/2013	Q1	Q2	Q3	Q4	Grand Total
Received	77	76	79	90	322
Compliant	75	76	67	53	271
Breach	2	0	12	37	51
% Compliance	**97.40%**	**100.00%**	**84.81%**	**58.89%**	**84.16%**

4.4. **Subject Access Requests:** during the year, the Trust received 3,819 requests for access to health records, an average of 318 per month. There were no breaches of the 40 calendar day response time. However, the Trust did receive two complaints via the regulator, the Information Commissioner, over the Trust's handling of subject access requests. One related to a patient's request for access to their health records and the other to a staff member's request for access to their personal data. In both instances, the Trust's investigation identified that the Trust had made some mistakes. These were rectified and procedures amended to minimise the risk of further breaches. In both instances, the regulator was satisfied with the actions that the Trust had taken and so refrained from taking regulatory action.

4.5. The Trust's FOI and Subject Access Request policies were both refreshed and ratified in March 2013. However, the Trust has invited the Information Commissioner's Office to conduct a consensual audit in the autumn in order to seek confirmation that its processes are robust and effective in minimising the risk of breaches. The audit will culminate with a three day on-site audit and formal report in September 2013.

5. Information Security Incidents

5.1. Staff are encouraged to report information governance risks and incidents. As table 4 overleaf shows there has been a steady rise in the number reported over the first nine months of the year, with the majority relating to the availability of health records. The decline in incidents occurring during the fourth quarter coincides with the introduction of the new radio frequency identification tagging system that has been applied to the health records. This has resulted in significant improvements in tracking and retrieving records in a timely manner.

Table 4: Information Security Incidents

2012/13	Q1	Q2	Q3	Q4	Total
Email	1	0	0	0	**1**
Health records	27	55	55	28	**165**
Post	1	1	2	9	**13**
Printer	1	0	0	1	**2**
Records Misfiled	2	0	0	0	**2**
Smartcards	4	3	6	2	**15**
Staff records	0	0	0	1	**1**
Verbal breach	0	1	1	1	**3**
Total	**36**	**60**	**64**	**42**	**202**

5.2. All except one incident were classified as level zero in accordance with DH guidance[1]. The remaining incident occurred in July 2012 and was graded at level 2. This was reported externally and involved the theft of a bag containing patient information from a clinician's car. The bag was recovered shortly afterwards by the police. An investigation was undertaken and a number of actions identified. These included a review of information governance training materials; inclusion of IG training uptake in Divisional key performance indicators; and quarterly reports on training uptake to the Management Board – Quality and Risk.

5.3. All of the above recommendations have been completed and 96.48% of staff completed their annual information governance training during 2012/2013.

6. Risk Management & Assurance

6.1. As well as line management responsibility for information governance staff, 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 team 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 and conducting regular information risk assessments.

6.3. The IT and IG managers facilitated a number of workshops with the IAOs to provide support in achieving these objectives. Whilst progress was made, the Trust recognises that further work is required to embed these processes. To

[1] Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents: Gateway Ref: 13177, DH Jan 2010

support this and other risk areas the IG Projects Lead will be retained until the end of October.

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 2013/14 are to:

7.3.1. promote and monitor the uptake of IG training which requires 95% of staff to undertake or refresh their training annually

7.3.2. work with Information Asset owners to embed effective information risk management activities as identified in 6.2 above

7.3.3. plan and undertake corporate records management audits in a minimum of four business areas

7.3.4. review and update the Trust's contract database to ensure third party contracts include relevant IG clauses

7.3.5. prepare for the ICO audit

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 auditor opinion. However, we recognise that continuous improvement is required and this is reflected in the retention of the IG Projects Lead for six months; the development plans outlined above; and the invitation to the ICO to audit how we are doing.

8.2. The Board is asked to receive and note this report.