Surrey and Sussex NHS
Healthcare NHS Trust

TRUST BOARD IN PUBLIC	**Date: 26th June 2014** **Agenda Item: 4.3**
REPORT TITLE:	Information Governance Annual report
EXECUTIVE PRESENTER:	Dr Des Holden Caldicott Guardian
EXECUTIVE SPONSOR:	Ian Mackenzie Director of Information & Facilities
REPORT AUTHOR:	Dipa Bhella Information Governance & Security Manager
REPORT DISCUSSED PREVIOUSLY: (name of sub-committee/group & date)	Information Governance Steering Group members: 30/05/2014

Action Required:

Approval ( )	**Discussion ( )**	**Assurance (√)**

Summary of Key Issues

- IG Toolkit Assessment 2013/14
- 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 – 26th June 2014

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 2014/15 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', each requirement must be scored at level 2 or above.

2.3. Prior to submitting its final assessment, the Trust's internal auditors, Baker Tilly, audited a random sample of 10 requirements based on the interim scores submitted by the Trust in October 2013. Based on the evidence available at the time of the audit, agreed the scores of seven of the requirements; three were overstated. In order to satisfy the requirements of the submitted scores additional evidence was uploaded before final submission.

2.4. In the year ending 31st March 2014, 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 (2013/2014)

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	9	0	9	66%	Satisfactory
Information Security Assurance	0	0	13	2	15	71%	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**	**38**	**7**	**45**	**71%**	**Satisfactory**

2.5. The Trusts results are comparable with four 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	40	5		45	70%	Satisfactory
BSUH	0	0	42	2	1	45	68%	Satisfactory
E. Sussex Healthcare	0	0	41	4		45	69%	Satisfactory
FPH	0	2	29	14		45	75%	Not Satisfactory
RSCH	0	0	35	10		45	74%	Satisfactory
SASH	0	0	38	7		45	71%	Satisfactory
Western Sussex Hospitals	0	1	33	11		45	74%	Not Satisfactory

*Not relevant

2.5.1. Frimley Park Hospital and Western Sussex Hospital were deemed ‘not satisfactory’ because they have requirements at level 1.

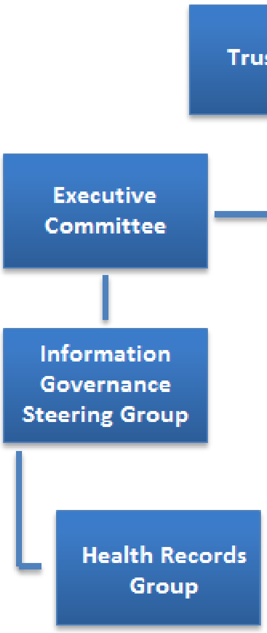
2.6. Information Governance Training: 96% of staff completed their annual information governance training during 2013/2014 this now needs to be refreshed for 2014/15. 95% of staff must complete their training each financial year, for the Trust to achieve level 2 in this requirement of the IG Toolkit assessment.

3. Assurance framework

3.1. The Trust's Information Governance Management Framework was reviewed in June 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 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. The Trust invited the Information Commissioner Office (ICO) between 10th and 12th September 2013 to conduct a consensual audit. The audit focused on three key areas; Information Governance Training and Awareness, Records Management and Requests for Personal Data.

The audit was conducted following the ICO's data protection audit methodology. The key elements of this were a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records. Their overall opinion was “On the basis of the work that we have performed we consider that the arrangements for data protection compliance in place at the Trust at the time, and within the scope, of the audit, with regard to data protection governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to”.

4.3. **Freedom of Information Requests**: The Trust received 571 FOI requests during 2013/14, a 44% increase on those received in the previous financial year. Despite this sharp increase in volume, the Trust has steadily improved its compliance with the 20 working day response time during the year, achieving an overall compliance rate of 80%.

4.4. **Table 3: FOIA Compliance**

2013/2014	**Q1**	**Q2**	**Q3**	**Q4**	**Grand Total**
Received	112	137	154	168	571
Compliant	82	105	126	146	459
Breach	30	32	28	22	112
% Compliance	**73%**	**77%**	**82%**	**87%**	**80%**

4.5 **Subject Access Requests:** In the year 2013/14 the Trust received 3269 enquiries relating to accessing health records (272 monthly average). However, only 37% of these enquiries resulted in formal requests (defined as a written request accompanied by the fee and satisfactory evidence of identity).

Of the 1192 valid requests received, 12% were from the patients themselves and 88% from third parties acting on behalf of the data subject. Compliance with the 40 day response time was 100%.

The Information Commissioner’s audit in September 2013 highlighted a number of recommendations to improve management of subject access requests (SARs). In response to this, we have:

- Developed a Medical records department page on the intranet to publicise the work of the team and the SAR process;
- Trained 28 staff from Human Resources, Customer Care, Medical Records, PGEC and Communication & Marketing teams on handling subject access requests;
- Revised standard letters and the SAR application form;

- Centralised the logging and management of SARs on the Trust's risk management system to improve reporting and governance arrangements; and
- Introduced an audit tool to sample the quality and legal compliance of response to SARs

The SAR policy is currently being revised and information on the SAR process, including the application form will be placed on our website shortly.

The introduction of these measures will improve governance arrangements; enable potential issues to be identified earlier; and improve visibility and performance monitoring.

5. Information Security Incidents

5.1. Staff are encouraged to report information governance risks and incidents. As table 4 below shows there has been a slight increase in the number reported in quarter 2, with the majority relating to the availability of medical records. The introduction of the new radio frequency identification tagging system that has been applied to the health records has shown a reduction in incidents reported compared to previous year figures.

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

2013/14	**Q1**	**Q2**	**Q3**	**Q4**	**Total**
Email	1	0	0	1	**2**
Health records / notes	33	48	24	31	**136**
Post	3	2	4	1	**10**
Printer / Fax	1	1	1	6	**9**
Removable media	0	0	0	1	**1**
Smartcards	0	0	1	1	**2**
Verbal breach	0	0	3	0	**3**
Other	1	0	2	0	**3**
Total	**39**	**51**	**35**	**41**	**166**

5.2.1 All except one incident were classified as level zero in accordance with DH guidance[1]. The remaining incident occurred in November 2013 and was graded at level 2. This was reported externally and involved a patient who had received documentation in error relating to four other patients receiving treatment at the Trust. The documentation was retrieved and the individuals affected were notified of the breach. An investigation was undertaken and actions identified, including a local review of processes for the management

[1] Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents Requiring Investigation: Version 2.0_June 2013

of sending letters internally and externally.

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, conducting regular information risk assessments, and ensuring staff have completed their annual information governance training.

6.3. The IG manager arranged one to one meetings with the IAOs to provide support in reviewing 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 2013/2014 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 2014/15 are to:

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

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

7.3.2.1. Develop an IG manual training booklet for those staff who do not access a computer whilst working at the Trust.

7.3.2.2. Develop an information portal for monitoring and reporting IG training compliance

7.3.3. Improve management of subject access 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 ICO auditor opinion.

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

Ian Mackenzie
Director of Information & Facilities
June 2014