University Hospitals Bristol NHS
NHS Foundation Trust

Information Governance Report for March 2013.

Information Governance (IG) is an overarching approach which helps University Hospitals Bristol NHS Foundation Trust to ensure that personal information is handled legally, securely, efficiently and effectively to support delivery of the Trust's strategic objectives.

Keys to the success of the Information Governance framework are:

- Dedicated information governance roles, including Executive Information Governance Lead, Senior Information Risk Owner, the Caldicott Guardian and Information Governance Manager
- Effective Information Governance policies and procedures
- A dedicated management group with responsibilities for information governance, e.g. the Information Governance Management Group or Risk Management Group.
- Training and Guidance to support all Trust Staff in the expected working practices;
- Incident Management processes and procedures to document any breaches and ensure learning from incidents.

This report describes the activities of the Trust on Information Governance over the last 12 months, together with the successes and challenges for the future

Information Governance Toolkit

The Information Governance Toolkit is an online tool that supports an organisation to self-assess its compliance against the Data Protection and Freedom of Information Acts alongside other statutory provisions and best practice guidelines.

The Trust published its evidence for Version 10 of the Information Governance Toolkit on the 31st March, 2013. The score was 68% the same as last year's score of 68%. However, the Trust is still red-rated with 3 requirements at Level 1. The IG toolkit is classified by whether the Trust has achieved Level 2 on all its requirements. Being red-rated is a consequence of having 3 requirements below level 2. This is a change from the previous year where we had one requirement at Level 0 and only 1 at level 1. The on-going challenge is to achieve 95% of staff trained in Information Governance: see below and Appendix for further detail.

Information Risk Management

Non-compliance with IG Toolkit requirement 209 'Overseas dataflow mapping' Level 1 in 2012/13

As many system managers are clinicians also, the requirement to produce documentation regarding Information Security has meant a steep learning curve with regard to identifying information risks and a general lack of understanding. Consequently the IG team has met individually with all system managers to produce required evidence.

The Internal IG auditor for Version 9 of the IG Toolkit (2011/12) had stated that all data flows should be mapped in order for the Trust to score Requirement 209 at a Level 2.

The Clinical Liaison and Information Systems Training Manager has been identifying systems in the Trust that hold Clinical Patient Identifiable Data (PID). Initially 265 systems in total were identified, of which 160 systems held Clinical PID, some of these systems are now redundant or duplications, which left 137 systems audited to assess future links to Medway. Information Governance has

followed up this audit with staff identified, but does need to link with all system managers and not just the systems holding Clinical PID; i.e. IG work needs to be done for the finance and HR systems equally as for PAS, RIS and Pathology.

Therefore, the IG Manager has been meeting with information system managers (IAAs) in the Divisions (initially it took an average of 4 hours per system) to gather the required information, as follows: -

a) Data Flow Maps – establishing what data is input to the system and also, what is extracted.

b) Access Controls – establishing whether the system meets the Trust standard for managing access.

c) Performing a Risk Assessment – establishing whether there are any risks that need to be escalated to the Information Asset Owner / Senior Information Risk Manager.

d) Business Continuity Plans – establishing whether the departmental BCPs also considered the issues in relation to the impact of loss of the IT system for any reason. If this has not already been done then either a quick system specific BCP is created or the IAA revises the departmental one.

e) At the same time we try to establish where any contracts are held.

Information Governance Training

Requirement 112, Level 1 2012/13

The Trust's IG training compliance peaked at 79 % in July / August 2012. The IG training materials had to be assessed by the national information governance toolkit team and they requested changes to achieve the required standard. These changes have been made included more detail with regard to clinical record keeping and information security plus there needs to be 10- 12 questions. A new booklet has been drafted and will need to be resubmitted for approval.

Confidential Data Sharing

Requirement 324, Level 1 2012/13

Any data shared for purposes other than direct patient care i.e. for secondary uses should be anonymised or pseudonymised, unless the patient has consented explicitly to the data sharing. This requirement sets out the steps that need to be taken in order to create a data safe haven and work is ongoing to implement the policy.

Internal Accountability / Responsibility

The Information Governance Management Group met 6 times in 2012/13. The Group is chaired by the Medical Director, who is also the Senior Information Risk Owner and attended by representatives of the Divisions, the Head of I M & T, the Caldicott Guardian and FOI/Data Protection Lead. The group oversees the development and approval of core Information Governance activities and the toolkit.

The SIRO verifies the score as 68%, see appendix for the IG Toolkit assessment Summary Report.

Internal Audit carried out an audit of the Information Governance Toolkit in February 2012 and the final report is included. Many of the issues raised have subsequently been addressed. The outstanding ones relate to those requirements not scored at Level 2.

Information Governance Serious Incidents.

There were no serious incidents reported to the Information Commissioner's Office during the period 2012/13. A list of incidents is included at appendix B.

Conclusion

The Trust maintained its position with regard to Information Governance and this year has maintained its overall score on the IG Toolkit.

Work continues with staff in the Trust to ensure that Information risks are identified and managed. Staff information governance awareness is improving with a resultant rise in enquiries and incidents reported.

A separate Freedom of Information Report is produced by the Freedom of Information lead.

University Hospitals Bristol NHS
NHS Foundation Trust

ACTION PLAN — APPENDIX A

Pg No.	Rec. No.	Recommendation	Risk Rating	Management Response	Manager Responsible	Action Date
6	R1	The Trust should implement a process for ensuring that only the relevant and up to date documentation is referenced to the Information Governance Toolkit.	Medium	Update July 2013 – All broken links identified and in process of being updated on Version 11 toolkit as part of toolkit review. To be completed prior to baseline publication 31st July, 2013. Hyperlinks identified as missing were updated. Produce a IG toolkit report in order to check hyperlinks to evidence which were not checked	L Nasey	Complete
6	R2	Business Continuity Plans should be reviewed, where necessary updated and SIRO approval obtained.	Medium	Update July 2013 – meeting held, LN to update BCP template to cover Information Governance / IT assets by Sept, 2013. IG manager to meet with Resilience Manager Emergency Planning.	LN/ Cass Sandmann	Complete
6	R3	Provide supporting documentation to explain the use of User Identity Management (UIM) combined with ESR to provide roles based access rights, rather than Registration Authority, for requirement 303.	Medium	Link was made prior to March 2012 publication of toolkit	LN	Complete
6	R4	Ensure that the introduction of the new training materials, once approved by Connect For Health, consolidates the use of the Essential Training booklet and all other Information Governance training provided with accurate staff training records.	Medium	Update July 2013 - This work will be completed by 26th July, 2013. On-going work. IG Toolkit report returned with some actions regarding training materials.	SDS	July 2013

University Hospitals Bristol NHS
NHS Foundation Trust

Appendix B – Information Governance Incidents in 2012/13

Incident Date	Cause Group	Cause 1	Details Of Incident
Jul-12	IG. Information Security	IG. Information Security	Hospital scan taken from a locker in a skip by member of the public
Jan-13	IG. Information Security	IG. Information Security	Patient files missing in office move
Jan-13	IG. Information Security	IG. Information Security	Loss of encrypted USB stick when travelling between 2 hospital sites
Mar-13	IG. Information Security	IG. Information Security	Ward handover sheet found outside hospital
Apr-12	IG. Patient Information	IG. Patient Confidentiality Breach	Dictaphone with clinic letter dictation lost from clinic room.
May-12	IG. Patient Information	IG. Mis-Sent Email / Letter / Fax (Patient In	Wrong discharge letter sent to patient
Apr-12	IG. Patient Information	IG. Loss / Theft Of Case / Handover Notes	Consultant lost his Dictaphone
Jun-12	IG. Patient Information	IG. Patient Confidentiality Breach	BBC camera crew were following a surgeon into another department, where a patient had not consented to filming.
Jun-12	IG. Patient Information	IG. Mis-Sent Email / Letter / Fax (Patient In	Fax mis-sent to Citizen's advice bureau who informed hospital
Jul-12	IG. Patient Information	IG. Mis-Sent Email / Letter / Fax (Patient In	2 different patient letters included in one envelope.
Jul-12	IG. Patient Information	IG. Patient Confidentiality Breach	Post trolley left unattended
Jul-12	IG. Patient Information	IG. Patient Confidentiality Breach	External contractor sent email from Hotmail to the Trust with patient information.
Sep-12	IG. Patient Information	IG. Patient Confidentiality Breach	Answerphone message left for patient (name only mentioned) on wrong number.
Sep-12	IG. Patient Information	IG. Loss / Theft Of Case / Handover Notes (Pa	Ex patient arrested by Devon and Cornwall police who had his hospital notes with him.
Sep-12	IG. Patient Information	IG. Patient Confidentiality Breach	Encrypted CD sent out with the password attached in breach of Trust policy.
Nov-12	IG. Patient Information	IG. Loss / Theft Of Case / Handover Notes (Pa	Patient handover list found outside hospital
Oct-12	IG. Patient Information	IG. Mis-Sent Email / Letter / Fax (Patient In	Patient copy notes sent via external mail to hospital but were not received
Nov-12	IG. Patient Information	IG. Patient Confidentiality Breach	Confidential patient information left at the counter of a local store. Patient information found by a customer and handed to a staff member at the local store.

Nov-12	IG. Patient Information	IG. Patient Confidentiality Breach	Wrong notes given to patient
Nov-12	IG. Information Security	IG. Policy Breach / Other	Member of staff rang from a non NHS company called HRA Research and Ethics (but on UHBristol IT network). The printer in their office is printing pathology reports for Dermatology skin cancer patients/nurse rosters/annual leave requests. IT network issue
Jan-13	IG. Patient Information	IG. Loss / Theft Of Case / Handover Notes (Pa	Printed ward handover sheet found in the Hospital site
Mar-13	IG. Information Security	IG. Policy Breach / Other	Clinician from another Trust was purchasing a drink, leaving patient notes to one side. Security reminded him to not leave confidential documents in public view and unattended.
Mar-13	IG. Patient Information	IG. Mis-Sent Email / Letter / Fax (Patient In	Fax mis-sent to GP surgery with same name but in different part of country.