NHS

Royal United Hospitals Bath
NHS Foundation Trust

Report to:	**Public Board of Directors**	**Agenda item:**	**16**
Date of Meeting:	**25 April 2018**		

Title of Report:	**Information Governance Toolkit Report**
Status:	**For Approval**
Board Sponsor:	**James Scott, Chief Executive**
Author:	**Dominique Emmanuel, Information Governance Manager**
Appendices	**Appendix 1: High Level Summary of 2018 Toolkit submission**

1. Purpose of Report (Including link to objectives)

Management Board and The Board are required to sign off the Trust's annual IG Toolkit return.

2. Summary of Key Issues for Discussion

The Information Governance Group agreed a target of 92% at the beginning of the year for the 2017/18 IG toolkit return to NHS Digital.

At the time of this paper being written for the Management Board, 45 of the 45 requirements have been completed and have achieved either level 2 or level 3. Therefore the trust overall score is 92% Satisfactory, Level 2. This is an increase of 2% on the previous year.

One area that is perhaps worthy of mention is the achievement this year of all staff having received annual mandatory training in Information Governance. A significant amount of work was put in by all Divisions and by all specialties to ensure that staff completed the training and the Information Governance team were grateful for the support given by Divisional managers and cascade trainers in particular.

An internal audit of the IG Toolkit was conducted this year by KPMG. Their final report issued on 28/03/2018 gave significant assurance with minor improvement opportunities.

3. Recommendations (Note, Approve, Discuss etc)

Request to note and approve the IG toolkit return by the Trust for 2017/18.

4. Care Quality Commission Outcomes (which apply)

The IG toolkit helps demonstrate compliance with Regulation 17 – Good governance.

5. Legal / Regulatory Implications (NHSLA / Value for Money Conclusion etc)

There are only two overall statuses for the IG toolkit which are satisfactory or unsatisfactory. Any requirements assessed only to have reached level 1(levels are from 0 to 3) means the Trust is graded as unsatisfactory. Our contracts with the CCG's require that we have reached a minimum of level 2 against all requirements of the toolkit and have a satisfactory grading. Achievement of level 2 minimum for the mandatory annual IG training of staff is important should their be any breaches of patient confidentiality as this is an area looked at by the Information Commissioners Office and would form part of their investigations.

6. NHS Constitution

This report shows that the Trust is committed to maintaining patient confidentiality and patient’s right to privacy, as well as complying with the Data Protection principles.

7. Risk (Threats or opportunities link to risk on register etc)

NA.

8. Resources Implications (Financial / staffing)

NA

9. Equality and Diversity

NA

10. Communication

NA.

11. References to previous reports

This information was first presented to the IG group on the 26th March 2018.

12. Freedom of Information

Public

Summary;

This year’s IG toolkit, version 14.1, has 45 separate requirements (please see Appendix 1).

At the time of this paper being written for the Management Board, all 45 requirements have been completed and have achieved either level 2 or level 3. The Trust overall score is 92% Satisfactory, Level 2. This is an increase of 2% on the previous year. A high-level summary of assessment against each indicator is attached as Appendix 1 for reference.

As mentioned, in March 2018 the Trust internal auditors (KPMG) conducted a detailed review of elements of the current year’s toolkit, as part of the assurance process. It reported the following good practice found;

- Structure: The Trust has an IG Manager, an IG Officer, a Senior Information Risk Officer (SIRO and a Caldicott Guardian (CG).
- The Trust has comprehensive approved IG policies in place. For example, concerning the completion and sign-off of the IG Toolkit, with associated implementation and improvement plans where necessary.
- A governance framework has been implemented to ensure that IG issues can be escalated to the most senior level of management, and during our review IG staff demonstrated a good understanding of their roles and responsibilities.
- The IG Group and other senior staff who are charged with Information Governance roles and responsibilities demonstrate sound understanding of their roles and responsibilities.
- IG training materials and guidance documents are in place. The Trust’s IG Toolkit training is delivered via face to face sessions and eLearning.
- The Trust conducts Information Risk Management Audit reviews in all business units. This is supported by the IRM Project Plan in order to identify all purposes supported by confidential personal information and determine the legal basis for each.

The requirement which merits recognition is the achievement of the requirement for all staff to have completed their mandatory IG training. This requirement was scrutinised as part of the KPMG audit. The achievement of this target came as a result of weekly compliance reports sent to all divisions to address performance in the poorest performing departments. A huge debt of gratitude goes to a number of cascade trainers who first undertook train the trainer learning and then went onto deliver a large number of local training sessions that were particularly accessible for nursing and medical staff who found it difficult to be released to attend core skills or other sessions in the Education Centre.

KPMG found 3 areas where minor improvements could be made:

- **IG Training -** The Trust has made significant progress in achieving the target 95% but does currently have a number of staff who have joined since April 2017 but not completed their IG Training. Recommendation – Establish al members of staff (including Bank staff) who have not completed their IG training but are currently working. Once this exercise has been completed, the Trust should look to ensure staff complete training as a priority.

- **Review and update policies/documents** – A policy review schedule should be implemented to ensure that key documentation uploaded to the toolkit is up to date and has been approved.

- **Completion and update of NHS Numbers Project Plan** - The Trust should create an action plan to ensure all systems are monitored and updated including the remaining non-compliant system (Tomcat) with associated completion dates. This may involve an updated analysis report to identify progresses made to previous years outstanding projects and to identify and monitor potential risks within systems on a yearly basis.

The Management Board are asked to support in view of the above;

- Thanks going to the cascade trainers and divisional managers who made such a significant effort to ensure all non- compliant staff completed their mandatory IG training allowing the Trust to achieve 95% of all staff trained in February 2018.

- That the Board and Management Board notes and approves the IG toolkit return score of 92%, Satisfactory, Level 2.

Appendix 1: **Version 14.1 (2017-2018) Assessment**

Requirements List

Req No	**Description**	**Status**	**Attainment Level**
Information Governance Management			
14.1-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	Confirmed Complete	Level 3
14.1-105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	Confirmed Complete	Level 3
14.1-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	Confirmed Complete	Level 3
14.1-111	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation	Confirmed Complete	Level 3
14.1-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	Confirmed Complete	Level 3
Confidentiality and Data Protection Assurance			
14.1-200	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation’s assessed needs	Confirmed Complete	Level 3
14.1-201	The organisation ensures that arrangements are in place to support and promote information sharing for coordinated and integrated care, and staff are provided with clear guidance on sharing information for care in an effective, secure and safe manner	Confirmed Complete	Level 3

14.1-202	Confidential personal information is only shared and used in a lawful manner and objections to the disclosure or use of this information are appropriately respected	Confirmed Complete	Level 3
14.1-203	Patients, service users and the public understand how personal information is used and shared for both direct and non-direct care, and are fully informed of their rights in relation to such use	Confirmed Complete	Level 3
14.1-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	Confirmed Complete	Level 2
14.1-206	Staff access to confidential personal information is monitored and audited. Where care records are held electronically, audit trail details about access to a record can be made available to the individual concerned on request	Confirmed Complete	Level 3
14.1-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	Confirmed Complete	Level 3
14.1-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	Confirmed Complete	Level 3
14.1-210	All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements	Confirmed Complete	Level 3
Information Security Assurance			
14.1-300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	Confirmed Complete	Level 3
14.1-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	Confirmed Complete	Level 3

14.1-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	Confirmed Complete	Level 3
14.1-303	There are established business processes and procedures that satisfy the organisation’s obligations as a Registration Authority	Confirmed Complete	Level 3
14.1-304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use	Confirmed Complete	Level 3
14.1-305	Operating and application information systems (under the organisation’s control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems	Confirmed Complete	Level 3
14.1-307	An effectively supported Senior Information Risk Owner takes ownership of the organisation’s information risk policy and information risk management strategy	Confirmed Complete	Level 3
14.1-308	All transfers of hardcopy and digital person identifiable and sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers	Confirmed Complete	Level 3
14.1-309	Business continuity plans are up to date and tested for all critical information assets (data processing facilities, communications services and data) and service - specific measures are in place	Confirmed Complete	Level 3
14.1-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	Confirmed Complete	Level 3
14.1-311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	Confirmed Complete	Level 3
14.1-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Confirmed Complete	Level 2
14.1-314	Policy and procedures ensure that mobile computing and teleworking are secure	Confirmed Complete	Level 3

14.1-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	Confirmed Complete	Level 3
14.1-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	Confirmed Complete	Level 2
Clinical Information Assurance			
14.1-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	Confirmed Complete	Level 3
14.1-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	Confirmed Complete	Level 2
14.1-402	Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care	Confirmed Complete	Level 3
14.1-404	A multi-professional audit of clinical records across all specialties has been undertaken	Confirmed Complete	Level 3
14.1-406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records	Confirmed Complete	Level 3
Secondary Use Assurance			
14.1-501	National data definitions, standards, values and data quality checks are incorporated within key systems and local documentation is updated as standards develop	Confirmed Complete	Level 3
14.1-502	External data quality reports are used for monitoring and improving data quality	Confirmed Complete	Level 2
14.1-504	Documented procedures are in place for using both local and national benchmarking to identify data quality issues and analyse trends in information over time, ensuring that large changes are investigated and explained	Confirmed Complete	Level 2
14.1-505	An audit of clinical coding, based on national standards, has been undertaken by a Clinical Classifications Service (CCS) approved clinical coding auditor within the last 12 months	Confirmed Complete	Level 2

14.1-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place	Confirmed Complete	Level 2
14.1-507	The secondary uses data quality assurance checks have been completed	Confirmed Complete	Level 2
14.1-508	Clinical/care staff are involved in quality checking information derived from the recording of clinical/care activity	Confirmed Complete	Level 2
14.1-510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national clinical coding standards	Confirmed Complete	Level 3
Corporate Information Assurance			
14.1-601	Documented and implemented procedures are in place for the effective management of corporate records	Confirmed Complete	Level 3
14.1-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	Confirmed Complete	Level 3
14.1-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken	Confirmed Complete	Level 3