Oxford University Hospitals
NHS Foundation Trust

Trust Board Meeting in Public: Wednesday 10 May 2017

TB2017.55

Title	**Information Governance and Data Quality Group Bi-annual Review**

Status	For discussion
History	Bi-annual update presented to TME on 13th April 2017

Board Lead(s)	Peter Knight, Chief Information & Digital Officer			
Key purpose	Strategy	**Assurance**	Policy	Performance

Executive Summary

1. The Trust received an overall rating of 99% following the final submission of the Information Governance toolkit scoring level 3 in 44 out of 45 standards.
2. Two serious information incidents were reported in the last 6 months of 2016/17, one incident was downgraded by the ICO.
3. 192 information governance incidents were reported in the second half of 2016/17. Five of these incidents resulted in minor harm and one was rated as moderate harm. The harm relates to the effect of the incident on the individuals concerned. The remaining 186 incidents were rated as no harm.
4. 217 FOI requests were processed in the second half of 2016/17, on average 69.6% were responded to within 20 working days.
5. The Trust has achieved a data validity score at the end of the Month 9 of 2016/17 of 99.1% against a national average of 96.5%.

Information Governance and Data Quality Group Bi-annual Review

Information Governance

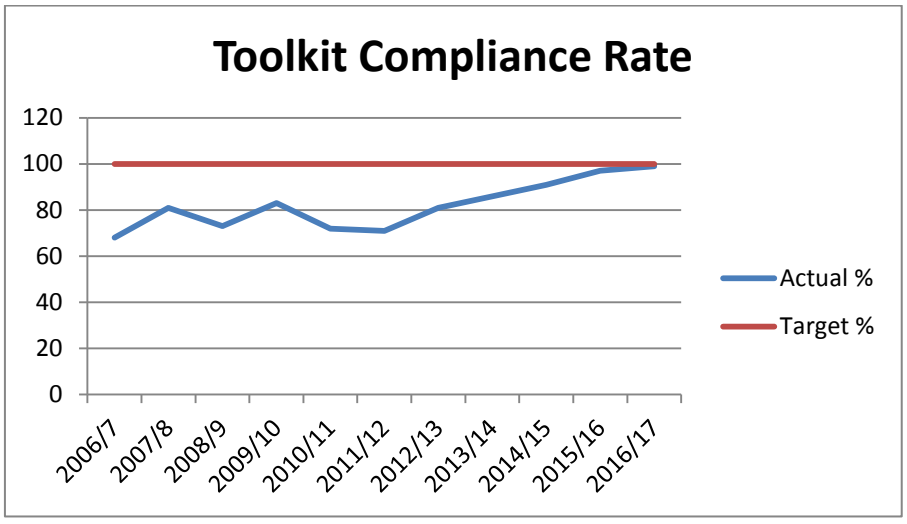
Introduction

1. This paper sets out the work which that been undertaken within the Information Governance Data Quality Group over the second six months of financial year 2016/17.

Information Governance Toolkit

2. In the second six months of financial year 20116/17 the Trust made two Information Governance Toolkit returns. The first in October 2016 where it was estimated that the Trust would return a compliance rate of 99%. The second return was at the end of this financial year on March 31st 2017. The finalized toolkit compliance rate was 99%. The Trust achieved a rating of level 3 in all attainment categories apart from 14-505 where level 2 was achieved. The criteria asked for evidence of coding accuracy which reached level 3. This requires that 95% accuracy is achieved in the coding of primary diagnosis and procedure. The main reason for not achieving 95% was coder error with staff not reviewing pre-assessment and referral documentation for elective cases due to workload. Coding will be reviewed in this area later on this year to check for improvement.

3. The Trust's annual Information Governance toolkit compliance rate for the past 10 years is presented below. The graph demonstrates that there has been a steady increase in compliance over the last five financial years. Oxford was one of the top performing Acute Trust's for Information Governance in the UK in financial year 2015/16.



4. The toolkit was audited in January 2017 by KPMG, nine standards were reviewed. Two recommendations were made which concerned the accuracy of documentation within the toolkit and training compliance. At the time of the audit the toolkit was still being updated, this included the removal of documentation from financial year 2015/16. An action plan was created to address training compliance. This will be monitored through the Information Governance Data Quality Group.

The Information Governance and Data Quality Group

5. The Information Governance Agenda and Data Quality Group (IGDQG) Meetings are chaired by the Caldicott Guardian and SIRO respectively. In the second half of 2016/17 the group has met four times.

6. The group is comprised of representatives from all Divisions and its remit is to support, strengthen and drive the data quality and information governance agendas within the Trust, ensuring the Trust complies with statutory responsibilities, fulfils its legal obligations in terms of confidentiality and data protection, and manages high quality information efficiently within a robust governance framework. Each Division holds local data quality meetings where highlights from both the data quality and information governance agendas are fed back.

7. The programme of information governance work is organized via an annual work programme which ensures that important objectives are met during the financial year. Progress against this work plan is presented in appendix two. The main highlight for the second half of this financial year has been the reconfiguration and re-launch of the information asset and data flow register. Feedback was received from staff following the launch of version one of the asset register in February 2016. The new version has been updated to include evidence that privacy impact and risk assessments have been conducted. The department are planning an on-going programme of contact with departments and communications to ensure that assets are logged.

8. The department's portfolio of work has continued to expand during the last six months of 2016/17 and closer working relationships with the IT department have been developed following the appointment of the Chief Information and Digital Officer. There has been greater emphasis on ensuring that privacy and system security are considered when new technologies are being purchased or there are changes in the way data is being managed through the completion of privacy impact assessments. The Information Governance department are also working more closely with the procurement department so that advice and support can be provided to staff before the purchase of systems where identifiable data is being processed or stored. The department is currently assisting with the procurement process for a new wheelchair management system. Work undertaken concerning Freedom of Information requests, subject access requests, incident and risk management is presented below.

9. During 2017, progress continues in ensuring that the data quality performance indicators are formally reviewed through IGDQG and the ratings are held on the Health Assure assurance tool with indicator owners responsible for uploading new or revised evidence.

10. The Data Quality Assurance Framework is underpinned by a programme of data quality audits undertaken by services themselves as well as by the Trust's own internal auditors and other external bodies. The results of these audits and the associated action plans are monitored at each meeting of the IGDQG.

11. The Trust Internal Data Quality Audit report achieved a result of significant assurance with minor improvement opportunities. All recommendations from the auditors and responses from within the Trust are monitored and tracked through the IGDQG to ensure compliance and completion.

12. The Trust also benchmarks its data quality performance using the Secondary User Service Data Quality Dashboard. The Trust performs strongly against both national benchmarks and local peer organisations achieving a data validity score at the end of the Month 9 of 2016/17 of 99.1% against a national average of 96.5%.

Information Governance Risks

13. Information governance risks are reviewed at every IGDQG meeting. There are currently three risks on the risk register.

    14.1 The Trust not having the resources, systems and/or processes to achieve and maintain level 2 on all requirements of the IG toolkit.
    14.2 Confidential Waste Management
    14.3 Misdirected patient letters

14. The Information Governance department is working closely with the Learning and Development department to improve training compliance by reducing the numbers of duplicate staff within the eLMS system by the use of NI numbers as unique identifiers. Furthermore, training will be able to be pass-ported from organizations in the new financial year improving compliance and reducing the need for staff to complete training in more than one organization.

15. The managed waste disposal service is still awaiting roll out on the John Radcliffe site. A site survey was conducted in early April. Waste bins are anticipated to be in place in April/May 2017.

16. The numbers of reported incidents of misdirected letters has increased in the last half of financial year 2016/17 with 39 incidents being reported as compared to 24 incidents in the first half of the year. This is an increase of 38%. Root cause analysis is undertaken on all reported incidents. The main root causes have been the manual misaddressing of envelopes and the stapling together of the wrong letter coversheet to the wrong letter due to the printing order of Cc letters from Alden. This latter problem is still being fixed by the company. An action plan is being completed by the transcription team which includes centralizing training for all transcription products and fixing the printing order of letter cover sheets

17. A new risk register is under construction which will list risks associated with information assets listed on the asset register.

Information Governance Incidents

Serious Incidents Requiring Investigation

18. Two incidents were reported to NHS Digital in the second half of 2016/17. When incidents are reported to NHS Digital via the Information Governance Toolkit, an automatic notification is sent to the ICO.

Incident Date	SIRI No	Detail	Status
22nd October 2016	2016/17-129	A patient was discharged with discharge documentation related to two other patients.	Complete. Downgraded from SIRI by the ICO.
13th January 2017	2016/17-142	Medical Records disclosed by the Subject Access Team to local authority without legal basis.	Under investigation. Reported to the ICO.

19. The first incident occurred in October 2016 to which the Trust was alerted in November following a formal complaint. A patient was discharged with documentation relating to two other patients, breaching confidentiality and the Data Protection Act 1998. The incident was reported

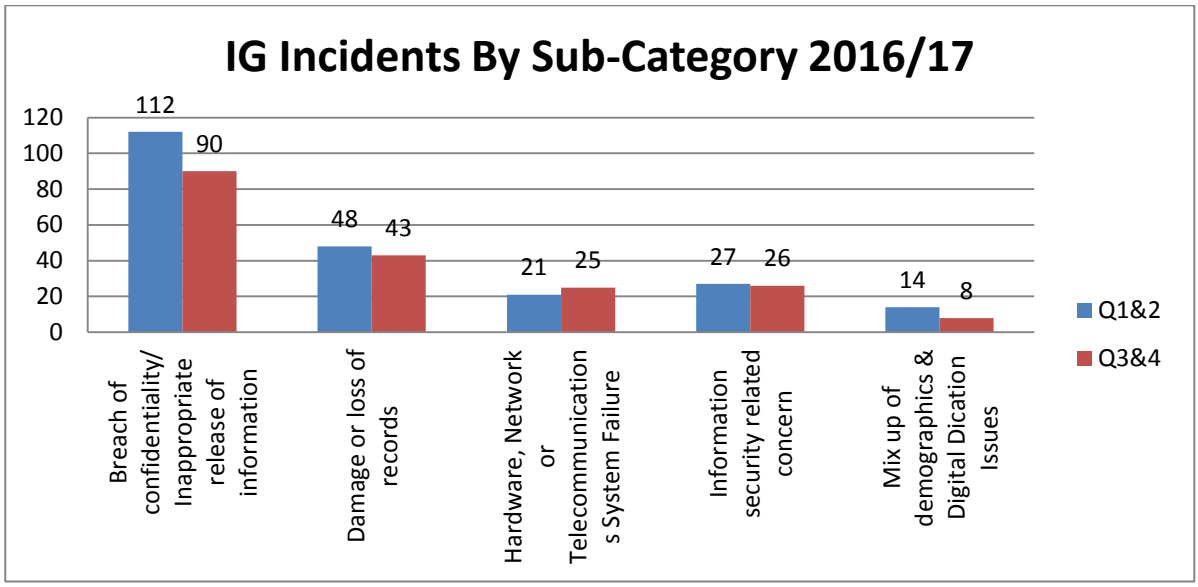
to the ICO, who felt that the incident did not warrant a SIRI investigation, and the incident was downgraded. The ICO asked the Trust to review staff training, and to emphasise to staff the importance of checking patient demographics. Divisional heads were contacted about the incident and asked to disseminate learning within their areas.

20. A local authority attempted to make a subject access request for a patient's records in relation to an application for housing. While the authority provided a consent form signed by the patient, the consent form did not cover accessing medical records, and so records were released to the authority without a legal basis. At the time of writing, this SIRI is in the latter stages of investigation. The incident has been reported to the Information Commissioner's Office.

Incidents

21. There were 192 incidents reported in the second 6 months of 2016/17. Information governance incidents are reported under the categories of consent, confidentiality, communications and information governance, and documentation and records (including EPR). The Information Governance Team is notified of all incidents reported under these categories but the responsibility for investigating these incidents remains with the department manager. However, where incidents are believed to be serious or require additional input the information governance team will assist staff.

22. The table below shows the number of incidents reported in the first and second halves of 2016/17 by sub-category.



23. The incident rate across these five sub-categories has remained broadly the same with a small increase in incidents reported concerning 'hardware, network, or telecommunications failure'. There has been a notable decrease in the numbers of incidents relating to breaches of confidentiality. Within the category 'breach of confidentiality/inappropriate' release of information, 39 incidents were misdirected letters, 10 incidents of discharge information given to the wrong patient, and 7 incidents of personal identifiable information found in locations accessible to the public. The primary causes for misdirected letters are machine errors in Letter Production, and lack of double checking of patient details when sending out clinical letters. The risk of giving discharge information to the wrong patient can be reduced by ensuring that patient demographics are checked and that paperwork matches with the patient being discharged. There were 5 instances of lost patient lists. These lists are generally found outside

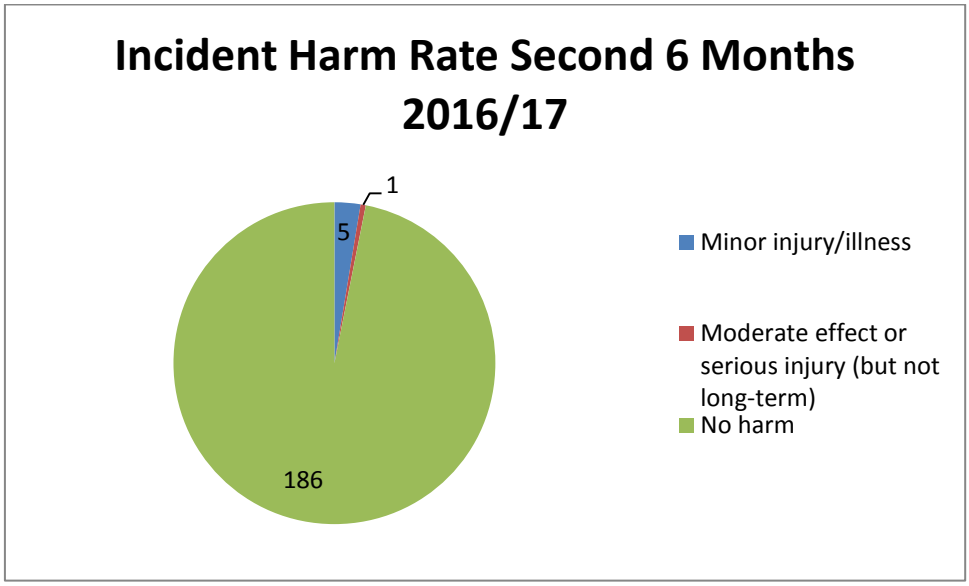
clinical departments. When patient lists have been found the Matron and/or the Clinical Lead are informed and asked to discuss at team meetings to ensure learning is shared, and that Trust guidance regarding the construction of patient lists is followed.

24. Analysis of incidents in the category, 'damage or loss of records,' shows the largest cause of incidents reported were missing notes (24), which could not be located prior to appointments or on admission. These were lost while in use within departments, in transit with inpatients to and from investigations in other departments with medical notes being left in the back of wheelchairs. This situation will be largely resolved following the introduction of paper-light working and scanning of notes as part of the Trust 'Go Digital' project. Three reported incidents related to poor documentation in records that led to confusion between staff affecting patient care.

25. No distinct trends were identified that related to information security concerns.

26. The main trend in incidents related to 'hardware, network, or telecommunications failure' is hardware failures that impacted on patient care, where staff were unable to prescribe, record observations, and register births on EPR.

27. The pie chart below shows the rate of harm caused by IG incidents. Most incidents reported resulted in no harm. Those incidents that caused minor harm mainly relate to the effect of the incident on the individuals concerned.



Subject Access Requests

28. The Data Protection Act 1998 provides the right to individuals to request copies of information that the Trust holds about them. Information requests are handled by two separate departments. Requests for medical records are processed by the Subject Access Request department and requests for all other information are processed by the IG department. The time-frame for responding to requests is 40 calendar days.

29. The table below sets out the requests for information made to the Information Governance department.

Status	Date of Application	Processing commenced	Brief description	Due Date (40th day)	Date sent	Within Timeframe?
Completed	2/11/2016	4/11/2016	Transcript from HR Hearing	12/12/2016	21/11/2016	Yes
Completed	16/11/2016	18/11/2016	HR File and all other correspondence	30/12/2016	10/01/2017	Request still ongoing
Completed	05/01/2017	05/01/2017	HR File	15/02/2017	15/02/2017	Yes
Completed	25/01/2017	25/01/2017	HR File and all other correspondence	06/03/2017	05/04/2017	No – timescales by applicant

30. The Information Governance department responded to 75% of requests within the statutory timescale.

31. The table below sets out the numbers of requests processed by the Subject Access Request department. The department is made up of three full time staff. At the time of writing some requests made in March are still within the 40 calendar day timescale.

Month – 2016	No. requests	Closed	Closed within 40 c/days
October	362	362 100%	347 95.86%
November	353	353 100%	321 90.93%
December	252	252 100%	232 92.06%
January	329	324 98.42%	309 93.92%
February	344	317 92.15%	304 99.37%
March	315	198 62.86%	198 62.86%
Total	1955	1806 92.38%	1711 87.92&

32. Obtaining information to complete requests can be challenging. A breakdown of issues is provided in the table below:

Issue	Background
Obtaining files	Patient currently attending Lost files
Consents for release	Files not returned to team within requested time frames *(usually due to secretariat holding onto files and not returning to team)*
Administration-audit monitoring, proof reading of records	Time consuming task each request as an average requires three different media type files to be processed and these can range from 1 to 15 volumes per media type to audit check.
Technological searches	Searches of system back-ups can be time consuming and yield large amounts of material.

IG cases - Information Commissioner's Office (ICO)

33. Two complaints were made to the ICO in the second half of 2016/17. The first complaint related to a failure to retain a copy of a referral letter sent to the Trust by a PCT in 2011. The Trust responded to the complainant and the matter was closed by the ICO with no further action.

34. The second complaint related to a freedom of information request regarding the disclosure of test results. The complaint was initially responded to in July 2016. However, the Trust were contacted by the ICO in December 2016 and asked to review legal arguments contained within the July response. The Trust provided a further response to the ICO in January 2017. The matter is still open.

Freedom of Information (FOI)

35. In the second half of financial year 2016/17 the department processed 217 FOI requests, this is a reduction of 24 requests (241) on the first half of the year. The statutory timeframe for responding to FOI requests is 20 working days. The average percentage rate for closure of requests within 20 working days is 69.6%; this is a 16% reduction from the first half of the year. The reason for this reduction in compliance with the 20 working day timeframe is the complexity of submitted requests related to Trust projects and a delay in receiving responses from Divisions.

36. FOI performance is presented below.

Month - 2016	Requests Received	Completed within 20 w/days	Completed out of 20 w/days	% within 20 w/days
October	58	42	16	72
November	37	30	7	81
December	35	30	5	86
January	44	28	16	63
February	43	21	23	49

37. In some cases the disclosure of information is exempted under FOI Act. The table below lists the exemptions invoked during the second 6 months of this financial year. The most commonly used exemption was s. 40. This exemption means that the Trust can refuse a request if it

relates to the disclosure of personal information concerning an individual. The most common example is the request of names of department heads by suppliers.

Oct – Mar 2016/17	
FOI exemption	**No of times used**
s.12 Exceeds the cost of compliance	2
s.22 Intended for future publication	2
s.40 Personal information	6
s.43 Commercial interests	3

38. Recent challenges for the department have been the number and complexity of FOI requests received concerning the Horton Maternity department and car parking at the John Radcliffe site. The department has been working closely with other corporate departments to process these requests.

Conclusion

39. This report summarises the highlights from the last six months. Progress continues to be made to reduce the information risk profile within the organization.

Nuala Buchan Brodie
Information Governance & Records Manager

Francine Tanner
Data Quality Programme Manager

May 2017

Appendix One – IG Toolkit Final Submission 2016/17

Version 14 (2016-2017) Assessment

Requirements List

Req No	Description	Status	Attainment Level
Information Governance Management			
14-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	Confirmed Complete	Level 3
14-105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	Confirmed Complete	Level 3
14-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	Confirmed Complete	Level 3
14-111	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
14-112	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			
14-200	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
14-201	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
14-202	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
14-203	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
14-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	Confirmed Complete	Level 3
14-206	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
14-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	Confirmed Complete	Level 3
14-209	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

14-210	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			
14-300	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
14-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	Confirmed Complete	Level 3
14-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	Confirmed Complete	Level 3
14-303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority	Confirmed Complete	Level 3
14-304	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
14-305	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
14-307	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
14-308	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
14-309	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
14-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	Confirmed Complete	Level 3
14-311	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
14-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Confirmed Complete	Level 3
14-314	Policy and procedures ensure that mobile computing and teleworking are secure	Confirmed Complete	Level 3
14-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	Confirmed Complete	Level 3
14-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	Confirmed Complete	Level 3
Clinical Information Assurance			

14-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	Confirmed Complete	Level 3
14-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	Confirmed Complete	Level 3
14-402	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
14-404	A multi-professional audit of clinical records across all specialties has been undertaken	Confirmed Complete	Level 3
14-406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records	Confirmed Complete	Level 3
Secondary Use Assurance			
14-501	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
14-502	External data quality reports are used for monitoring and improving data quality	Confirmed Complete	Level 3
14-504	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 3
14-505	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
14-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place	Confirmed Complete	Level 3
14-507	The secondary uses data quality assurance checks have been completed	Confirmed Complete	Level 3
14-508	Clinical/care staff are involved in quality checking information derived from the recording of clinical/care activity	Confirmed Complete	Level 3
14-510	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			
14-601	Documented and implemented procedures are in place for the effective management of corporate records	Confirmed Complete	Level 3
14-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	Confirmed Complete	Level 3
14-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken	Confirmed Complete	Level 3

Appendix Two

Information Governance Work Programme 2016/17 March 2017 v10

Task	Toolkit Ref	Date	Lead	Status
Approve 2016-17 work programme		April	NB-B	G
Review IG Risks and update Health Assure		Monthly	NB-B	On-going
Review of IGTK V13 results		April	NB-B	G
Review asset register, and asset risk register	301	July, Oct, Jan, April	NB-B	G No review in Jan as new asset register under construction
Complete Trust-wide information mapping exercise	308	April onwards	NB-B	On-going
Review IG Training Needs Analysis and Develop Training Plan including review of workbook, assessment and training compliance.	111, 112	April onwards	NB-B	G
Trust wide audit of corporate records (in at least 4 corporate areas)	604	Oct - March	NB-B	G
Review and update Publication Scheme	603	July, Oct, Jan, April	VG	On-going
IGTK V14 baseline submission score	All	July, October	NB-B	G
IGTK v14 Updates to IGDQ	All	Aug, Nov, Apr	NB-B	On-going
Approval of IGTK v14 final submission score	All	March	NB-B	G
Carry out spot checks to confirm staff understanding of IG responsibilities	111, 112	On-going	NB-B /SP/V G	G
Undertake service user satisfaction survey	203	February	NB-B	G
Undertake staff user survey	201	February	NB-B	G
IG Incidents/Confidentiality Breaches Updates to IGDQ		Monthly	NB-B	On-going
Review of IG Key Documents Programme 2016/17	101	Monthly	NB-B	On-going

Task	Toolkit Ref	Date	Lead	Status
ICO News Releases Update to IGDQ		Monthly	NB-B	On-going
FOI performance update to IGDQ		Monthly	NB-B	On-going
IG bi-annual report / SIRO report to the Audit Committee **(to include FOI, Data Quality Section)** and then to Trust Board, to include IG overview from 15/16, toolkit submission, the management of information risk.	307	Bi-annually (April/October)	NB-B /FT/PP	G
Bi-Annual Subject Access Request Report (combined SAR / IG Team)	205	Oct/Apr	BW / RH	G
Complete annual IG Assurance Statement before submission of the toolkit.		March 2017	NB-B /PK/C B	G