Oxford University Hospitals NHS
NHS Foundation Trust

Trust Board Meeting in Public: Wednesday 11 May 2016

TB2016.53

Title	**Information Governance Data Quality Group Bi-Annual Review**

Status	For discussion
History	Bi-annual Update

Board Lead(s)	**Mr Andrew Stevens, Director of Planning & Information**			
Key purpose	Strategy	**Assurance**	Policy	Performance

Executive Summary

1. The Information Governance toolkit was submitted on the 31st March 2016. The compliance rate for the Trust is 97% with 42 out if 45 standards scoring level 3 with the remaining 3 scoring level 2.
2. 222 information governance incidents were reported in the second half of 2015/16. Five of these incidents resulted in minor harm with the remaining 197 incidents rated as no harm.
3. A Trust Cyber Security Task Force has been established to focus on improving security and managing cyber security risks.
4. The Trust Internal Data Quality Audit report achieved a result of significant assurance.
5. The Trust has achieved a data validity score at the end of the Month 10 of 2015/16 of 99.1% against a national average of 96.2%.
6. 290 freedom of information requests were made to the Trust in the second half of this financial year. The percentage of requests responded to within 20 working days was on average 88%.
7. **Recommendation** The Trust Board is asked to note this report.

Information Governance (IG) Bi-Annual Review

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 2015/16.

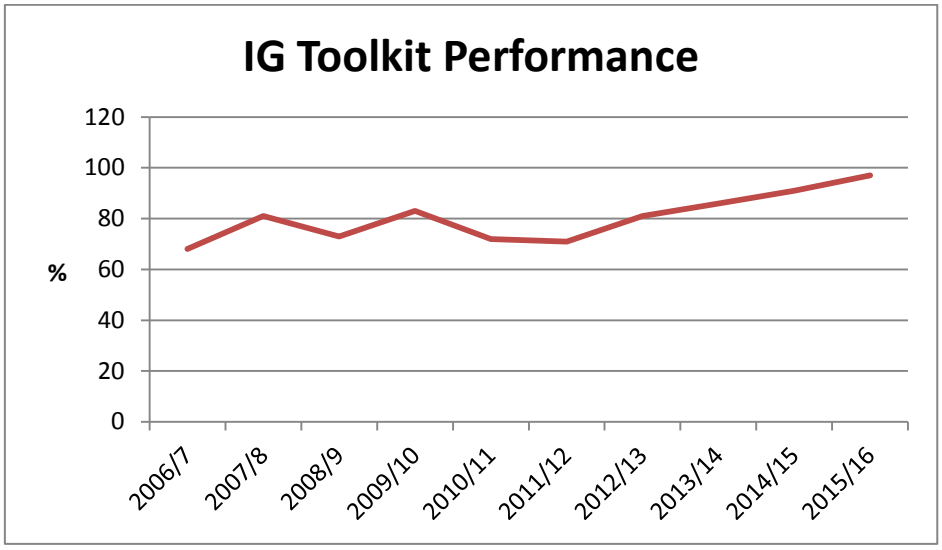
Information Governance Toolkit

2. The Information Governance Toolkit comprises of a collection of information governance standards drawn from central guidance and Department of Health Policy. Organizations that process patient data are required to carry out self-assessments of their compliance which are grouped under the following headings:

   2.1 Information governance management
   2.2 Confidentiality and data protection assurance
   2.3 Information security assurance
   2.4 Clinical information assurance
   2.5 Secondary use assurance
   2.6 Corporate information assurance

3. The toolkit enables organizations to measure their compliance against these standards and provides a framework for attainment and continuing improvement. Toolkit standards are owned by subject specialists within the organization who work in conjunction with the Information Governance team to provide the final submission of evidence.

4. Three assessments are undertaken against these standards during the course of a financial year. An initial baseline score which is submitted at the end of July, a mid-year update score at the end of October and a final published score at the end of March. The Trust toolkit self-assessment scores for the past 10 years are presented below.



5. The table demonstrates that there has been a steady increase in compliance over the last four financial years. The Trust's overall rating was satisfactory. Forty two out of forty five parameters scored level 3 with three areas scoring level 2. Plans are in place to increase performance for standards scoring level 2.

6. The toolkit is audited annually by KPMG. An audit was conducted in October 2015 which showed partial assurance with improvements required. At the time the audit was being conducted the department was subject to a number of staff changes. The Information Governance Manager was on maternity leave and the Freedom of Information Officer transferred jobs to become the Information Governance Officer leaving a vacancy until October 2015. The department was re-audited in March 2016 and the Trust was given a rating of significant assurance with minor improvement opportunities.

Information Governance Data Quality Group

7. It is the role of the Information Governance Data Quality group to oversee the work of the information governance department. The overall board lead is the Senior Information Risk Officer (SIRO) who is Chair of the Data Quality section of the meeting. The Information Governance section of the meeting is Chaired by the Trust Caldicott Guardian. Meetings have moved from being six weekly to monthly and in 2015/16 the group met nine times. 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.

8. The programme of information governance work is organized via an annual work programme which ensures that important objectives are met during the financial year. End of year progress against this work plan is presented in appendix two. Significant progress was made this year in regard to outstanding projects. An on-line Information Asset Register was developed to provide a central repository for assets within the Trust and a review of contracts was undertaken to ensure that they contained the correct information governance clauses. Feedback from KPMG indicated that other providers have struggled to achieve these objectives.

9. At the heart of the Trust's data quality approach is the data quality assurance framework. Under this framework the data underpinning all of the key performance indicators included in the Integrated Performance Framework are given a two component rating by the Information Governance and Data Quality Group. The first component of the rating is a ranking on a scale of 1-5 to reflect the level of assurance that is available around the data quality. The second component comprises a traffic light rating to indicate the level of data quality that the assurance mechanisms have found.

10. The ratings for all indicators are reviewed informally by the indicator owners on a quarterly basis. Any proposed changes have to be approved by the IGDQG. In addition, the ratings of all indicators are formally considered on an annual rolling basis by the IGDQG. At these formal reviews, the indicator owners are required to

present the evidence supporting the proposed rating for the data underpinning each indicator to the IGDQG. The IGDQG then considers the evidence and rates it against the framework.

11. During 2015/16, progress continues in ensuring that the evidence supporting each rating is held on the Health Assure assurance tool with indicator owners responsible for uploading new or revised evidence

12. 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.

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

14. 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 10 of 2015/16 of 99.1% against a national average of 96.2%.

Information Governance Risks

15. Currently the risk register is comprised of three global information governance risks.
    - 15.1 The Trust not having the resources, systems and/or processes to achieve and maintain level 2 on all requirements of the IG toolkit.
    - 15.2 Breach of confidentiality or loss of data leading to a serious incident or ICO investigation
    - 15.3 Confidential Waste Management

16. A risk review was undertaken in the second half of 2015/16. The objective of the risk review was to identify Trust wide strategies to mitigate the most pressing information governance risks. The top four risks were identified as Email/Fax/Letter sent to wrong person, Information inappropriately shared with 3rd party, mixed up patient notes and handover list found. Risk assessments are being undertaken and immediate actions to mitigate these risks have been initiated.

17. Work has been undertaken through the development of the new Information Asset Register to understand the risks related to assets and information flows within the organization. The Asset Register requires those completing it to assess the risk to their asset or information flow of the risk of confidentiality breach, data loss, asset failure and loss and risk to patient care of asset failure and loss. Risks to assets and flows will be discussed quarterly at the Information Governance and Data Quality Group and will be added to a specially designated risk register. This will provide the SIRO with a fuller understanding of the risk carried by the organization.

18. A programme of spot checks has also been carried out to identify any immediate risks to the organization. Forty two spot checks of clinical areas were carried out in total. No immediate causes for concern were identified although practice was variable in different areas. A top ten good practice advice sheet will be issued to clinical areas and spot checks will continue in 2016/17 with a report being issued concerning improvements that are required to department managers.

Information Governance Incidents

Serious Incidents Requiring Investigation

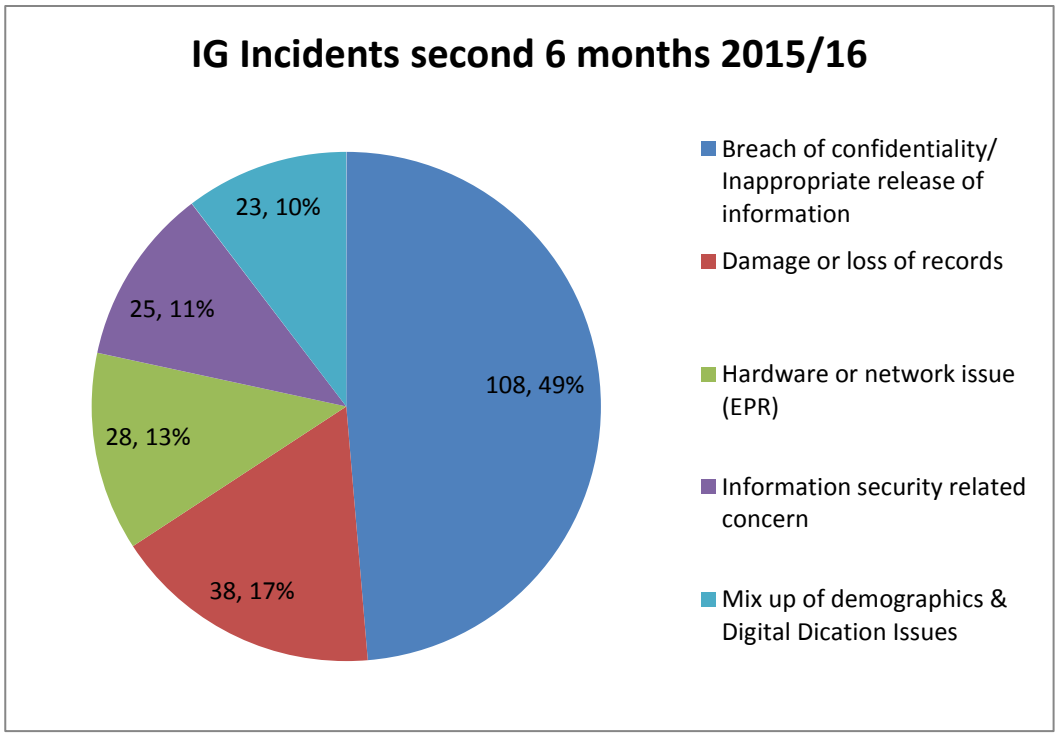
19. Two incidents were reported to the Information Commissioner in the second six months of 2015/16.

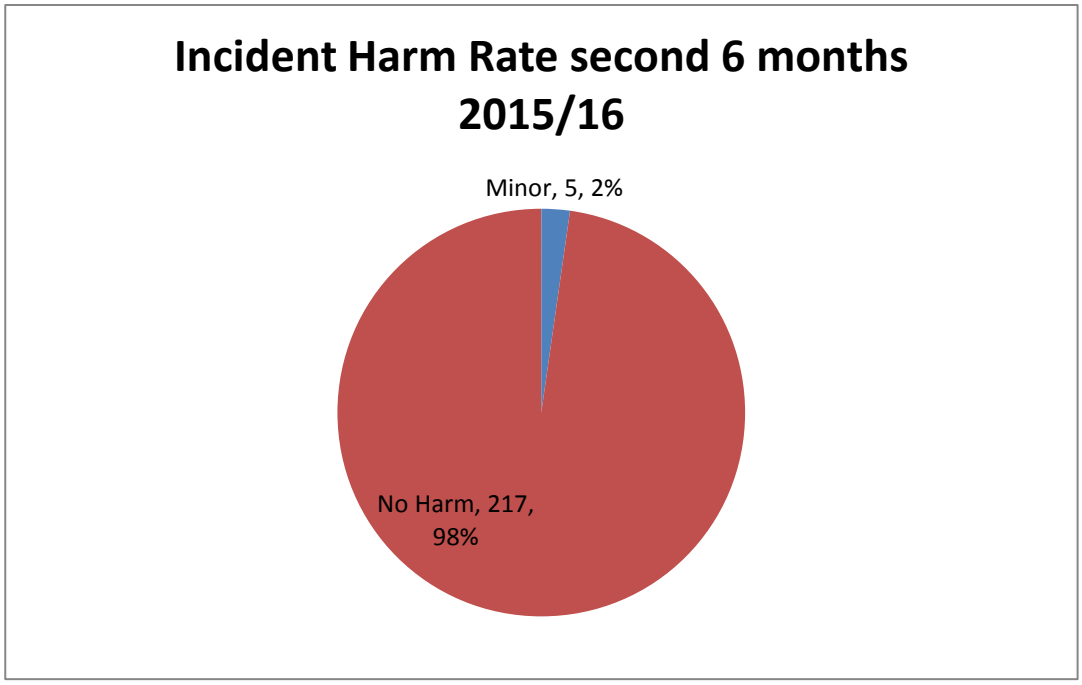
Incident Date	SIRI No	Detail	Status
12-Jan-16	2016/009	Lost diary in community	Closed by the Information Commissioner
26-Jan-16	2016/014	Misfiled letter in maternity notes	Under investigation

Incidents

20. There were 222 incidents reported in the last 6 months of 2015/16. Incidents were reported under the categories of consent, confidentiality, communications and information governance, documentation and records (including EPR) are reported to the department leads as well as the information governance team. The responsibility for investigating these incidents remains with the departmental manager. However, where incidents are believed to be serious or require additional input the information governance team will assist with investigations.

21. The tables presented below shows the ratio of incidents reported and their harm rate for these two categories.





22. The majority of incidents that were reported resulted in no harm. There was no identifiable trend associated with incidents rated as minor harm. Work is underway to reduce the use of patient lists within the organization. A tender process has been completed which will improve how confidential waste is handled and confidential waste bins will be changed Trust wide. A risk assessment is also underway to reduce the risk of sending mail to the wrong recipient.

Cases Involving the Information Commissioner's Office (ICO)

23. Two complaints were made to the ICO in the second half of 2015/16. No formal action has been taken by the ICO other than referring the complaints back to the Trust to be addressed. The complaints related to a failure to receive all information requested - Sept 2015 and inaccurate information within the Spine portal - Sept 2015.

Freedom of Information

24. The department recruited a new full time FOI Officer who started work in October 2015. Compliance with the 20 working day statutory deadline has increased since their appointment and the average response rate is 88%. This is a 19% increase on the same period in 2014/15.

25. Detail concerning FOI performance is presented below.

Performance 2015/16	Oct	Nov	Dec	Jan	Feb	Mar	
# FOI Requests Received	92	30	50	50	46	22	
Sent within 20 days	70	26	48	48	40	18	
%	76%	86%	96%	96%	86%	90%	
Not within 20 days	22	4	2	2	6	4	
%	24%	13%	4%	4%	13%	18%	
Reasons for breaching 20 day response target							

26. The vast majority of requests continue to come from journalists and private companies with significant additional requests from researchers both inside and outside the NHS. The most popular topics for requests are agency expenditure, delayed transfer of care rates and vacancy rates.

Cyber Security

27. In August 2014 KPMG undertook a Cyber Security Audit of the Trust. The purpose of the audit was to assess the maturity of cyber controls against government standards in combination with internationally accepted maturity models.

28. The Trust has established a Cyber Security Task force to focus on improving security and managing cyber security risks. The current plans include measures to improve password security, to ensure secure network log-ons as well as improving the endpoint security across the trust. New advance firewalls have been installed and web security measures have been enhanced. In addition innovative security software from a Cambridge start-up is being trialled. External independent intrusion detection and vulnerability will be assessed during this trial and an action plan will be developed to counter any threats uncovered during the trial.

29. Regular update reports are submitted to the Audit Committee.

Conclusion

30. This report summarises the key issues from the last six months. Significant progress has been made resulting in improvements to information governance compliance, data quality and IT security within the Trust. Plans have been established to ensure continued improvement throughout the next financial year.

31. The Trust Board is asked to note this report.

Nuala Buchan Brodie
Information Governance & Records Manager

Francine Tanner
Data Quality Programme Manager

John Skinner
Director IM&T

27 April 2016

Appendix One – IG Toolkit Final Submission 2015/16

Req No	Description	Status	Attainment Level
Information Governance Management			
13-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	Confirmed Complete	Level 3
13-105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	Confirmed Complete	Level 3
13-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	Confirmed Complete	Level 3
13-111	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
13-112	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			
13-200	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
13-201	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
13-202	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
13-203	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
13-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	Confirmed Complete	Level 3
13-206	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
13-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	Confirmed Complete	Level 3
13-209	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
13-210	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			

13-300	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
13-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	Confirmed Complete	Level 3
13-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	Confirmed Complete	Level 3
13-303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority	Confirmed Complete	Level 3
13-304	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
13-305	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
13-307	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
13-308	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
13-309	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
13-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	Confirmed Complete	Level 3
13-311	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
13-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Confirmed Complete	Level 3
13-314	Policy and procedures ensure that mobile computing and teleworking are secure	Confirmed Complete	Level 3
13-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	Confirmed Complete	Level 2
13-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	Confirmed Complete	Level 2
Clinical Information Assurance			
13-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	Confirmed Complete	Level 3
13-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	Confirmed Complete	Level 3
13-402	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

13-404	A multi-professional audit of clinical records across all specialties has been undertaken	Confirmed Complete	Level 3
13-406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records	Confirmed Complete	Level 3
Secondary Use Assurance			
13-501	National data definitions, standards, values and validation programmes are incorporated within key systems and local documentation is updated as standards develop	Confirmed Complete	Level 3
13-502	External data quality reports are used for monitoring and improving data quality	Confirmed Complete	Level 3
13-504	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
13-505	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 3
13-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place	Confirmed Complete	Level 3
13-507	The Completeness and Validity check for data has been completed and passed	Confirmed Complete	Level 3
13-508	Clinical/care staff are involved in validating information derived from the recording of clinical/care activity	Confirmed Complete	Level 3
13-510	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			
13-601	Documented and implemented procedures are in place for the effective management of corporate records	Confirmed Complete	Level 3
13-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	Confirmed Complete	Level 3
13-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken	Confirmed Complete	Level 2

Appendix Two

Information Governance Work Programme 2015/16 Final Version

Task	Toolkit Ref	Date	Lead	Status
Approve 2015-16 work programme		April	NB-B	G
Review IG Risks and update Health Assure		April, July, Oct, Jan	NB-B	On-going
Review of IGTK V12 results		April	NB-B	G
Assess compliance against the recommendations made by *"Information: to share or not to share?"* (The Caldicott 2 report) March 2013		July, October, March	NB-B	A
Review IG policies and procedures, approve at IGDQG	101	On-going, see appendix 1	CB/ NB-B	On-going
Create comprehensive list of contractors and third parties that have access to information and/or information assets. Ensure contracts reviewed annually.	110, 302	April - December	NB-B	G
Review information asset register, reviewing possibility of a new system to record assets, and associated data flows	301	April - March	NB-B	G
Assessment of transfers of personally identifiable information to countries outside the UK. *Transfers should be fully documented, reviewed and tested to ensure compliance with the DPA and the IG tool kit.*	301	April - March	NB-B	A
Complete Trust-wide information mapping exercise	308	April onwards	NB-B	A
Review IG Training Needs Assessment and Develop Training Plan including review of workbook and assessment	111, 112	April onwards	NB-B	A
Plan audit of corporate records (in at least 4 corporate areas)	604	August - December	NB-B	G
Review and update Trust Privacy Statement and HR Privacy Statement		August	CB / NB-B	A
Review and update Publication Scheme	603		VG	A
Review of use of fax machines within the Trust (from IGDQ minute 13-14/009) Project team established		April onwards	CB	A
IGTK V13 baseline submission score	All	July, October	NB-B	G

Task	Toolkit Ref	Date	Lead	Status
Approval of IGTK V13 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 /TM/VG	G
Undertake service user satisfaction survey	203	September	NB-B	G
Undertake staff user survey	201	September	NB-B	G
EPR Implementation Updates to IGDQ		6 weekly	PA	On-going
RA Updates to IGDQ (to include annual audit to cover smartcards, RA hardware (computers, scanners and smartcard readers) and consumables.	303, 304	6 weekly	HJ	On-going
IG Incidents/Confidentiality Breaches Updates to IGDQ		6 weekly	NB-B	On-going
Review of IG Key Documents Programme 2015/16		6 weekly	NB-B	On-going
ICO News Releases Update to IGDQ		6 weekly	NB-B	On-going
FOI performance update to IGDQ		Quarterly (June, Sept, Dec, Mar)	NB-B	On-going
IG bi-annual report / SIRO report to the Health Informatics 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	A
Annual Subject Access Request Report (combined SAR / IG Team)	205	April, October	BW / RH	A
Review and update evidence for all level 3 toolkit requirements		April onwards	NB-B	On-going
Discuss information assets and risks quarterly at IGDQG	310	March 2015 meeting onwards.	NB-B	On-going
Complete annual IG Assurance Statement before submission of the toolkit.		March 2016	NB-B /AS/CB	On-going