Oxford University Hospitals
NHS Foundation Trust

Trust Board Meeting in Public: Wednesday 9 May 2018

TB2018.50

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

Status	For discussion
History	This paper has been discussed at TME and Audit Committee

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

Executive Summary

1. The Trust's has obtained a score of 100% and satisfactory at its final submission on 28 March 2018.

2. Four serious information incidents were reported in the financial year of 2017/18. Two of these were reported in each half of the financial year.

3. 136 information governance incidents were reported in the second half of 2017/2018. One incident resulted in harm caused, 12 were reported as 'near miss'. The remaining 123 resulted in no harm.

4. 398 FOI requests were received in the second half of 2017/18, on average 79% were responded to within 20 working days. This is a slight reduction from 86% in the first half of the year, and likely related to a reduction in staffing levels within the Information Governance department.

5. 70% of requests for copy medical notes were completed within the statutory 40 calendar day timeframe. No requests for electronic (non-health records) were completed within this timescale due to the complexity and scope of requests along with the time taken to identify and prepare the information for disclosure.

6. The Trust has achieved a data validity score at the end of the Month 9 of 2017/18 of 98.9% against a national average of 96.5%.

Information Governance and Data Quality Group Bi-annual Review

Information Governance

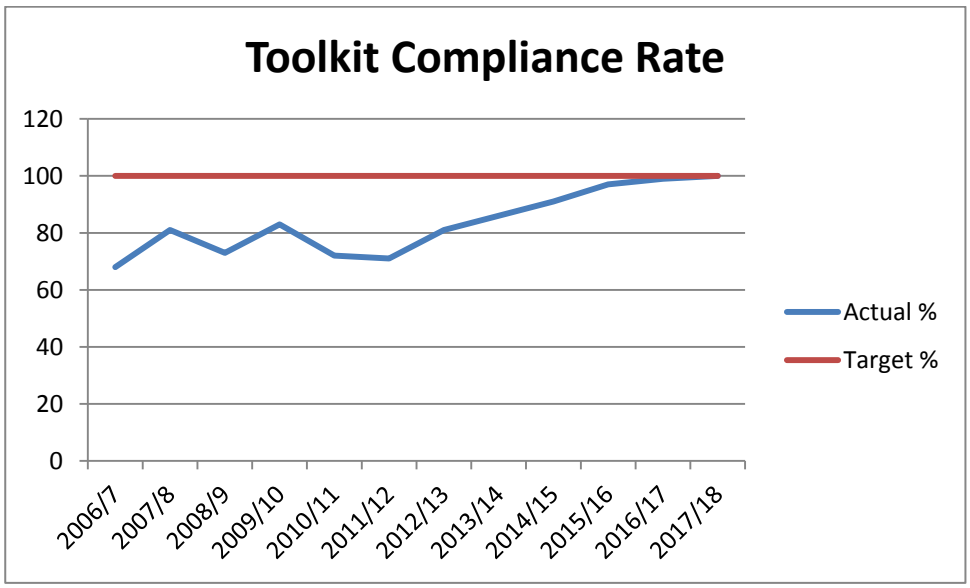
Introduction

1. This paper sets out the work which that been undertaken by the Information Governance Data Quality Group over the second six months of financial year 2017/18.

Information Governance Toolkit

2. In the final six months of financial year 2017/18 the Trust made one Information Governance Toolkit return at the end of March 2018. The toolkit's final compliance rate is 100% and satisfactory, see appendix one. The Trust continues to be the best performing Acute Trust for Information Governance compliance in the country for the 3rd year running.

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.



4. The toolkit is audited annually by KPMG. An audit was conducted in early January 2018. Eight standards were selected for audit. Over the past six months the department has undertaken significant work to address areas of the toolkit that required additional input. The use of a unique identifier within the e-learning management system was approved to reduce duplicate entries within the system; this has yet to go live while Data Protection Impact Assessments are undertaken.

5. The Information Governance training module has been reviewed and expanded to ensure staff have a more comprehensive, practical understanding of data protection. Induction training has been refined to incorporate examples of previous data breaches and steps that can be taken to reduce similar issues arising in future. In addition, the Information Governance team has been liaising with divisional leads to address any concerns relating to General Data Protection Regulation (GDPR) compliance.

The Information Governance and Data Quality Group

6. The Information Governance and Data Quality Group (IGDQG) meetings are chaired by the Caldicott Guardian and SIRO respectively. In the second half of 2017/18 the group has met four times.

7. 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. The group's main purpose is to ensure that the Trust complies with its legal obligations in terms of confidentiality and data protection, and that it 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 discussed. An 'at a glance' document is produced following each meeting for dissemination within Divisions.

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. Progress against this work plan is presented in appendix two. The main highlight for the second half of this financial year has been the review of Information Governance policies and procedures to ensure that the Trust is prepared for the forthcoming change in data protection law In addition, promotion of the Information Asset Register has been undertaken to document data assets, as well as the importance of completing Data Protection Impact Assessments (DPIA's), both are compulsory under the new legislation.

9. The department has continued to undertake and review its action plan to ensure that it is prepared for the enactment of the GDPR and associated domestic legislation. Actions have included updating the Trust's privacy statements for patients and staff and developing a statement for children, re-writing the Trust's existing policy for data requests and expanding this to include data portability along with ensuring that internal processes are GDPR compliant. The department is already reviewing information assets which have been successfully documented on the information asset register. However, a reduction in staffing combined with an increase in Subject Access Requests (SARs) has delayed approval of several recent information assets. In addition to extensive departmental visits, the Information Governance team will continue their programme of communications in the form of electronic messages, fact sheets and leaflets for staff and patients.

10. Throughout 2018 progress continues in ensuring that the data quality performance indicators are reviewed through the Information Governance Data Quality Group. Each domain is formally reviewed annually whilst all indicator owners are required to undertake an informal review on a quarterly basis. The data quality rating has two components; the first component has a five point rating which assesses the level and nature of assurance that is available in relation to a specific set of data. The second component of the overall rating is a traffic-light rating to indicate the level of data quality found through any auditing/benchmarking. The ratings are held on the Health Assure assurance tool with indicator owners responsible for uploading new or revised evidence.

11. The Data Quality Assurance Framework is underpinned by a programme of compulsory 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 divisional data quality meeting as well as at the IGDQG.

12. The Trust benchmarks its data quality performance using the Secondary User Service Data Quality Dashboard. We continue to perform strongly against both national benchmarks and local peer organisations achieving a data validity score at the end of the Month 9 of 2017/18 of 98.9% against a national average of 96.5%.

13. A verbal overview of cyber security is presented at each meeting. Details of current cyber security work are contained within a separate report to the Audit Committee.

Information Governance Risks

14. Information governance risks are reviewed quarterly at the IGDQG meeting. There are currently four risks on the risk register.

    12.1 Confidential Waste Management
    12.2 Misdirected patient letters
    12.3 Information governance training compliance
    12.4 Unregistered information assets and data transfers

15. Locked confidential waste bins have been rolled out across all Trust sites reducing the risk significantly of data loss. This remains on the register temporarily owing to some bins becoming full quickly and the need to reassess confidential waste provision in these areas.

16. The misdirection of letters remains a risk to the organization. Attempts were made in the first half of 2017/18 to roll out a software fix but this was unsuccessful and had to be recalled. Root cause analysis is being undertaken for all reported incidents concerning the misdirection of letters. The Trust is currently trialling digital dictation directly into the Cerner record, the trial is going well and it is hoped that following large scale roll-out of this project this risk should reduce significantly.

17. Information governance training compliance, discussed in paragraph four and unregistered information assets and data transfers are risks which have been added to the register in the first half of this financial year. The on-line asset register has now been completed. The register format has been amended to include PIA questions to ensure GDPR compliance. This resulted in a pause in promoting the register. This work has now been completed and the register will continue to be promoted. Information risk management training has been uploaded to the eLMS training site, the SIRO will be writing to all asset owners in the Trust setting out their responsibilities and asking for completion of the training.

18. No information asset risks have been identified following reviews of the asset register.

Information Governance Incidents

Serious Incidents Requiring Investigation

19. Two incidents were reported to NHS Digital in the second half of 2017/18. When incidents are reported to NHS Digital via the Information Governance Toolkit, an automatic notification is sent to the Information Commissioner's Office (ICO).

Incident Date	SIRI No	Detail	Status
November 2017	1718-065	Two clinical letters containing sensitive medical information were stapled together and sent in error	Completed
March 2018	1718-092	An unencrypted memory stick containing patient data was lost at a London conference	Under investigation

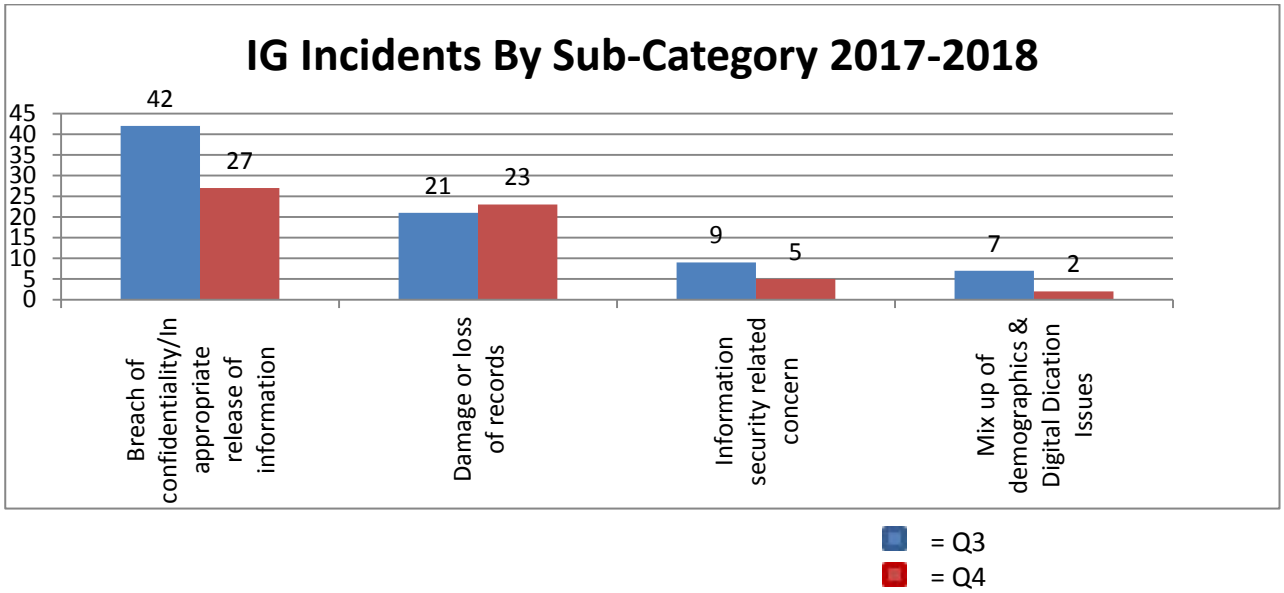
20. The first incident involved a staff member erroneously stapling two letters together which contained sensitive medical information. The incident was reported to the ICO and actions were taken to mitigate the risk of similar issues arising in future. These actions included reminding staff to remain diligent when reviewing correspondence, and updating the Trust's Standard Operating Procedure regarding the processing of patient letters.

21. The second incident regarded a staff member losing an unencrypted memory stick used during a presentation at a London conference. The ICO have been notified and the issue remains under investigation.

Incidents

22. There were 136 incidents reported in the second half of 2017/18, a decrease from the 143 incidents reported in the two preceding financial quarters. 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.

23. The table below shows the number of incidents reported in the second half of 2017/18 by sub-category.



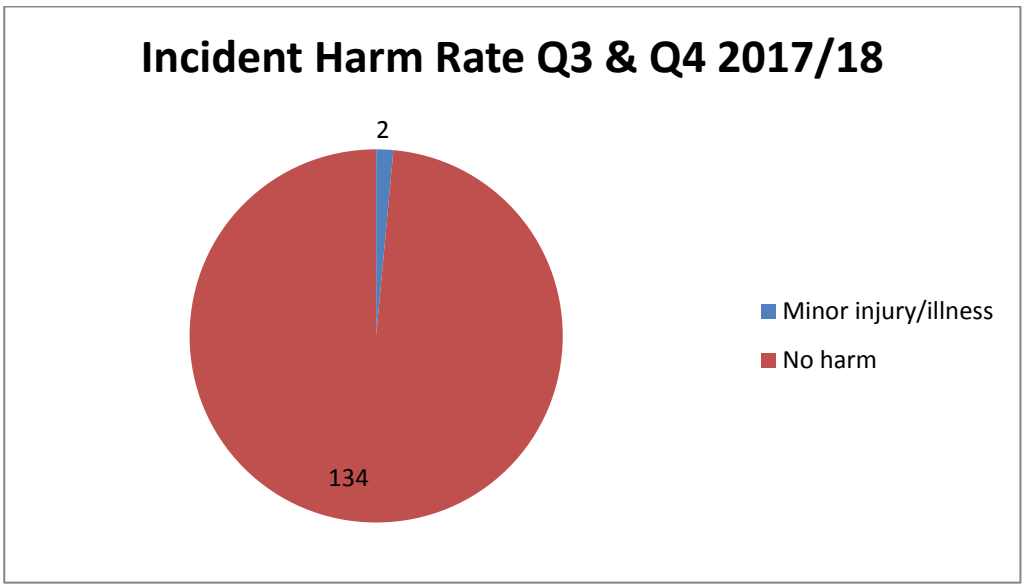
24. The incident rate across these four sub-categories has fallen except in the 'damage or loss of records' category where numbers of incidents have slightly increased. The fall in incidents is particularly noticeable in the 'breach of confidentiality' category where 42 incidents were reported in Q3, compared with 27 incidents reported in Q4.

25. Analysis of incidents of the category 'breach of confidentiality' shows the largest category of incidents reported was communications sent to the wrong recipient (33) out of the 69 breaches of confidentiality. These include clinic letters with the incorrect cover sheet stapled to the letter, and are the result of human error. All incidents undergo appropriate levels of investigation. Some incidents relate to envelope stuffing errors in letter production when sending out clinic/appointment letters. The root cause in this instance has been machine error.

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

27. There were 44 incidents reported related to 'damage or loss of records', 30 of these incidents were related to loss of records, with the majority being medical notes.

28. 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 related to the effect of the incident on the individuals concerned.



Subject Access Requests

29. The Data Protection Act 1998 provides the right for individuals to request copies of information that the Trust holds about them. The majority of information requests are handled by two separate departments, although other departments such as Radiology, Occupational Health and the Legal department ~~can~~ handle~~d~~ ad-hoc requests. Requests for medical records are generally processed by the Subject Access Request department and requests for information not related to health records are processed by the IG department. The time-frame for responding to requests is 40 calendar days. The response time will change to one month with effect from 25th May when the GDPR comes into effect.

30. 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?
Pending	6th October	11th October	Search of documents for data subject	20th November	n/a	No
Complete	20th October	20th October	Search of documents for data subject	29th November	29th November	Yes

Status	Date of Application	Processing commenced	Brief description	Due Date (40th day)	Date sent	Within Timeframe?
Complete	8th November	8th November	Search of documents for data subject	18th December	1st December	Yes
Complete	23rd November	28th November	Search of documents for data subject	2nd January	21st December	Yes
Complete	27th November	11th December	Search of documents for data subject	20th January	17th January	Yes
Pending	22nd December	22nd December	Search of documents for data subject	31st January	13th February	No
Pending	13th February	13th February	Search of documents for data subject	23rd March	n/a	No
Pending	14th March	14th March	Search of documents for data subject	23rd April	n/a	

31. The Information Governance department responded to 50% of requests within the statutory timescale. Two requests were received following the reduction of IG staff levels due to maternity leave. One request has resulted in the largest non-medical request that the Trust has received, and has required in excess of 100 hours work.

32. The department has procured additional Adobe Acrobat Pro licences increase the department's capacity for redacting information. A vacancy within the team affected the team's ability to complete requests within the statutory time scale.

33. Under the forthcoming General Data Protection Relations (GDPR) the timescale for completing requests will be lowered to one month, but requests can be refused if they are 'manifestly unreasonable'.

34. 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 who have each processed on average 621 requests for information during the second half of this financial year. The department closed 97.53% of all requests received. The average percentage closure rate within the statutory timescale was 87%.

Period	Requests	Closed	Closed within 40 days
2017/07 (Oct)	277	277 100%	191 68.96%
2017/08 (Nov)	358	358 100%	266 74.31%
2017/08 (Dec)	261	260 99.82%	224 85.83%
2017/09 (Jan)	315	308 97.78%	229 72.70%
2017/10 (Feb)	282	216 76.60%	192 68.09%
2017/11 (March)	326	174 53.37%	174 53.38%
Totals	3862	3410 88.30%	2893 74.91%

35. Vacancies in the team were a contributing factor resulting in requests being closed outside the statutory time frame. The table below sets out in more detail why request deadlines were not met in some cases.

Issue	Background	Action
Staff shortage	Senior Staff member left the Trust at the end of June	Recruited new member of staff who commenced 02.10.17
Staff annual leave	Only one full time member of staff working on requests given the additional absence of the Senior Staff member.	As above
Recruitment to Band 3 post	Due to recruitment issues to this post the senior administrative staff within this team have had to support the Band 3 administration tasks.	Post filled-starting date 14th May 2018
Obtaining physiotherapy files for copying	No administrative staff in these areas to support this work	Continued problems with off-site locations.

IG cases - Information Commissioner's Office (ICO)

36. One complaint was made to the ICO from a service user, and one issue was raised by the Trust. Both issues has subsequently been reviewed and closed with the ICO.

Date	Complaint	Outcome	Status
8th March	**COM0715397** A clinical letter containing sensitive personal data was disclosed to another patient	Upheld – ICO recommendation to review verification measures for letter checking, and provide refresher training to staff.	Closed
29th March	**RFA0713700** A subject access request was not completed within the 40 day response time.	Partially upheld – The Trust did not provide the required data within 40 days, but the requestor was unwilling to refine the scope of their request.	Closed

Freedom of Information (FOI)

37. In the second half of financial year 2017/18 the department processed 398 FOI requests, a significant rise from the 266 received in the last half of financial year 2016/17. The statutory timeframe for responding to FOI requests is 20 working days. National events have fuelled part of this increase, events such as the topic of Weinstein sexual harassment case, and the save the Horton campaign. In the second half of financial year 2017/18 the average percentage rate for closure of requests within 20 working days was 79%, a decrease from 86% in the preceding two financial quarters. The main reasons for not meeting the 20 working day timeframe are complex requests that cross departments and delays in sign-off from divisions or executives prior to SIRO sign-off.

38. FOI performance is presented below. Percentages completed within 20 working days do not include requests that are awaiting clarification, as 20 working days have not expired thus compliance cannot be measured. The total of number of requests processed excluding requests awaiting clarification are shown in the table below.

Month – 2017-2018	Requests Received	Completed within 20 w/days	Completed out of 20 w/days	% within 20 w/days
October	72	58	14	80.5
November	69	51	18	73.9
December	49	37	12	75.5
January	72	42	30	58.3
February	71	58	13	81.6
March	65	12	0 at time of report	18.4 at time of report
Total	326	258	87	79.1

39. In some cases the disclosure of information is exempted under FOI Act. The table below lists the exemptions used during the final 6 months of this financial year. The most commonly used exemption is s.40. This exemption means that the Trust can refuse a request if it is for personal data, such as a staff member's name or email address.

October 2017 – March 2018		
FOI exemption		**No of times used**
s.12	Exceeds the appropriate limit (18 hours work).	35
s.14(2)	Repeated request.	3
s.21	Information is readily accessible (in the public domain).	2
s.22	Information intended for future publication.	1
s.31(1)(a)	Release of information likely to prejudice the prevention or detection of crime.	3
s.40	Personal data.	39
s.43	Release of information likely to prejudice commercial interests.	26

40. The FOI department received two requests for internal review in the final six months of 2017/18. The first internal review was to consider whether an FOI exemption was engaged appropriately. The verdict was that the exemption applied was appropriate, however more information about the basis on which the exemption was applied would have been helpful.
41. The second internal review related to the redacting of a requested document and inadequacy of the Trust's response. The verdict was that the document had been redacted appropriately, however additional information should have been provided in response to the requestor's question.

42. Recent challenges for the department have been the increase in numbers of FOI requests received, combined with a reduction in staffing levels. The department has widened its accumulative knowledge of the exemptions and exceptions within the FOI legislation to reduce the burden that FOI places on the Trust. The departments purchase of a software package which began use in September, has allowed for greater analysis of prominent trends in subject matter or organisations making repeated requests.

October 2017 – March 2018
Requests exceeding 20 working days

Month FOI received	Delay of 1-2 working days	Delay of 3-6 working days	Delay of 7-13 working days	Delay of 14+ working days
October	5	5	1	5
November	1	8	2	5
December	5	3	2	2
January	10	8	6	7
February	3	4	5	1
March	0	0	0	0
Total	24	28	16	20

43. When requests are not completed within 20 working days, a large portion are completed within 1-2 working days after the deadline, and a smaller proportion completed 3-6 working days after the deadline has passed. Over the six month period the numbers of requests exceeding the deadline has increased, due to several requiring review by multiple departments, the communications team, and/or legal counsel.

October 2017 – March 2018
Reasons for requests exceeding 20 working days

Month FOI received	Signoff Delays	Departmental Delays	Complexity Delay
October	3	5	8
November	7	8	3
December	2	5	5
January	5	17	9
February	2	6	6
March	0 at time of report	0 at time of report	0 at time of report
Total	19	41	31

44. Delays in responding to requestors usually have three root causes. Delays in departments responding to the request is the largest cause of delay, this can be because the data is not readily accessible. This can have a domino effect in delaying sign-off from divisional managers and executive directors which is the next biggest factor in responses being delayed. Some responses are delayed because of the complexity of the request, particularly requests which cover two or more departments. The FOI Team are constantly working to improve relationships with departments and help departments to determine quickly what data exists and where ownership lies.

Conclusion

45. This report summarises the highlights from the last six months. Progress continues to be made to embed processes and preparation continues for the up-coming change in data protection legislation. New challenges exist concerning the governance and use of Cloud solutions. The Information Governance department is working with the IM&T department to resolve this. Meeting the statutory timeframe for disclosure of non-health records has proved challenging due to the size of requests and the requirement to extract and seek consent for release of electronic information from multiple locations and personnel. The new data protection legislation coming into force in May 2018 should ease this situation and will allow the Trust to refuse requests deemed manifestly unreasonable and require applicants to collaborate with the organization to find a workable solution to facilitate their information request.

    A staffing plan is in place in order that the Trust continues to meet its Information Governance requirements. This will include a greater emphasis on cyber security, as reflected in the updated Information Governance Toolkit. These changes are aligned with the Review of Data Security, Consent and Opt-Outs submitted by the National Data Guardian.

Russell Dean
Information Governance Officer

Simon Pillinger
Information Governance Officer

Francine Tanner
Data Quality Programme Manager

9th April 2018

Appendix One – IG Toolkit end of year submission 2017/18

Version 14.1 (2017-2018) Assessment

Report Results

Information Governance Management										
Assessment	**Stage**	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Total Req'ts**	**Overall Score**	**Self-assessed Grade**	**Reviewed Grade**	**Reason for Change of Grade**
Version 14.1 (2017-2018)	Baseline	0	0	3	2	5	80%	Satisfactory	n/a	n/a
	Performance Update	0	0	3	2	5	80%	Satisfactory	n/a	n/a
	Published	0	0	0	5	5	100%	Satisfactory	n/a	n/a
	Target	0	0	0	5	5	100%	Satisfactory	n/a	n/a

Confidentiality and Data Protection Assurance										
Assessment	**Stage**	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Total Req'ts**	**Overall Score**	**Self-assessed Grade**	**Reviewed Grade**	**Reason for Change of Grade**
Version 14.1 (2017-2018)	Baseline	0	0	4	5	9	85%	Satisfactory	n/a	n/a
	Performance Update	0	0	4	5	9	85%	Satisfactory	n/a	n/a
	Published	0	0	0	9	9	100%	Satisfactory	n/a	n/a
	Target	0	0	0	9	9	100%	Satisfactory	n/a	n/a

Information Security Assurance										
Assessment	**Stage**	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Total Req'ts**	**Overall Score**	**Self-assessed Grade**	**Reviewed Grade**	**Reason for Change of Grade**
Version 14.1 (2017-2018)	Baseline	0	0	10	5	15	77%	Satisfactory	n/a	n/a
	Performance Update	0	0	10	5	15	77%	Satisfactory	n/a	n/a
	Published	0	0	0	15	15	100%	Satisfactory	n/a	n/a
	Target	0	0	0	15	15	100%	Satisfactory	n/a	n/a

Clinical Information Assurance										
Assessment	**Stage**	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Total Req'ts**	**Overall Score**	**Self-assessed Grade**	**Reviewed Grade**	**Reason for Change of Grade**
Version 14.1 (2017-2018)	Baseline	0	0	1	4	5	93%	Satisfactory	n/a	n/a
	Performance Update	0	0	1	4	5	93%	Satisfactory	n/a	n/a
	Published	0	0	0	5	5	100%	Satisfactory	n/a	n/a
	Target	0	0	0	5	5	100%	Satisfactory	n/a	n/a

Secondary Use Assurance										
Assessment	**Stage**	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Total Req'ts**	**Overall Score**	**Self-assessed Grade**	**Reviewed Grade**	**Reason for Change of Grade**
Version 14.1 (2017-2018)	Baseline	0	0	5	3	8	79%	Satisfactory	n/a	n/a
	Performance Update	0	0	5	3	8	79%	Satisfactory	n/a	n/a
	Published	0	0	0	8	8	100%	Satisfactory	n/a	n/a
	Target	0	0	0	8	8	100%	Satisfactory	n/a	n/a

Corporate Information Assurance										
Assessment	**Stage**	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Total Req'ts**	**Overall Score**	**Self-assessed Grade**	**Reviewed Grade**	**Reason for Change of Grade**
Version 14.1 (2017-2018)	Baseline	0	0	2	1	3	77%	Satisfactory	n/a	n/a
	Performance Update	0	0	2	1	3	77%	Satisfactory	n/a	n/a
	Published	0	0	0	3	3	100%	Satisfactory	n/a	n/a
	Target	0	0	0	3	3	100%	Satisfactory	n/a	n/a

Overall										
Assessment	**Stage**	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Total Req'ts**	**Overall Score**	**Self-assessed Grade**	**Reviewed Grade**	**Reason for Change of Grade**
Version 14.1 (2017-2018)	Baseline	0	0	25	20	45	81%	Satisfactory	n/a	n/a
	Performance Update	0	0	25	20	45	81%	Satisfactory	n/a	n/a
	Published	0	0	0	45	45	100%	Satisfactory	n/a	n/a
	Target	0	0	0	45	45	100%	Satisfactory	n/a	n/a

Grade Key

Not Satisfactory	Not evidenced Attainment Level 2 or above on all requirements (Version 8 or after)
Satisfactory with Improvement Plan	Not evidenced Attainment Level 2 or above on all requirements but improvement actions provided (Version 8 or after)
Satisfactory	Evidenced Attainment Level 2 or above on all requirements (Version 8 or after)

Appendix Two

Information Governance Work Programme 2017/18 November 2017 v4

Task	Detail	date start	due date for completion	complete?
PIA for searches of staff activity	Complete criteria for staff activity searches	14/08/2017	18/08/2017	Y
	Complete criteria document for P2Sentinal searches.	14/08/2017	18/08/2017	Y
Review PIA policy and process.	First draft.	14/08/2017	25/08/2017	Y
	Work on final daft.	28/08/2017	08/09/2017	Y
	Prepare for September IGDQ.	11/09/2017	13/09/2017	Y
Write FOI Procedure.	Write FOI Procedure & present to October IGDQG	21/08/2017	13/09/2017	Y
Select FOI Management system	Review options.	17/04/2017	28/04/2017	Y
	PIA on selected system.			
	Test system.	14/08/2017	25/08/2017	Y
Risk register review quarterly.	Q1	05/06/2017	09/06/2017	Y
	Q2	04/09/2017	08/09/2017	Y
	Q3	04/12/2017	08/12/2017	
	Q4	29/01/2018	02/02/2018	
SAR Report	November	30/10/2017	03/11/2017	Y
	March	19/02/2018	23/02/2018	Y
Quarterly Spot Check Audits	Q1	19/06/2017	23/06/2017	Y
	Q2	18/09/2017	29/09/2017	Y
	Q3	20/11/2017	24/11/2017	Y
	Q4	22/01/2018	26/01/2018	Y
Quarterly Corporate Records audit.	Q1			
	Q2			
	Q3	04/12/2017	08/12/2017	Y
	Q4	29/01/2018	02/02/2018	

Task	Detail	date start	due date for completion	complete?
Bi-annual Toolkit review to IGDQG.	November	02/10/2017	20/10/2017	Y
	March	05/02/2018	17/02/2018	Y
Review of Assets and Flows	Q1	01/07/2017	31/07/2017	Y
	Q2	04/09/2017	29/09/2017	Y
	Q3	13/11/2017	07/12/2017	Y
	Q4	19/02/2018	23/02/2018	Y
Update guidance on logging information assets		14/08/2017	18/08/2017	Y
Create log of information sharing agreements.		01/04/2017	31/03/2018	
Information risk training is uploaded onto ELMS		01/08/2017	14/11/2017	Y
Tidy your systems week.	Liaise with server team			
Corporate Records Policy	Review current policy.	14/08/2017	18/08/2017	Y
	Research best practise.	14/08/2017	18/08/2017	Y
	Draft policy	14/08/2017	25/08/2017	Y
	Prepare for IGDQG	01/12/2017	13/12/2017	
	Any additional work	28/08/2017	22/09/2017	Y
	Present to October IGDQG	25/09/2017	20/12/2017	
Procurement Workstreams	Obtain access to Oracle	11/09/2017	15/09/2017	Y
	Review of contracts using PID	09/10/2017	30/11/2017	
	IG guidance for procurement process	02/10/2017	31/03/2018	Y
Training	Follow-up NHSP, temp and contractor training.	14/08/2017	25/08/2017	Y
	Training needs analysis	28/08/2017	13/12/2017	
Surveys	Staff awareness - Write	18/12/2017	22/12/2017	
	Staff awareness - Run survey	08/01/2018	23/02/2018	
	Staff awareness - Prepare for IGDQG	26/02/2018	02/03/2018	
	Service User - Write	18/12/2017	22/12/2017	

Task	Detail	date start	due date for completion	complete?
	Service User - Run survey	08/01/2018	23/02/2018	
	Service User - Prepare for IGDQG	26/02/2018	02/03/2018	
GDPR	Write briefing paper		30/06/2017	Y
	Staff Briefing email	02/10/2017	30/04/2018	
	Divisional/directorate staff briefings	02/10/2017	31/12/2017	Y
	Draft privacy notice - must include the right to be forgotten.	20/10/2017	15/11/2017	
	Addition of opt-out option - this must be able to pull info from SCR	18/09/2017	11/10/2017	Y
	Consult with children concerning draft privacy notice	29/01/2018	30/03/2018	
	Write staff process for patients making a request for deletion of their information.	23/10/2017	31/12/2017	
	Place prominent notice on Trust website advising patients of their information rights	01/04/2018	18/05/2018	
	Explore whether access to patient portal satisfies right to portability.	09/10/2017	20/10/2017	Y
	Update information Trust intranet concerning data portability & subject access.	01/04/2018	18/05/2018	
	Update incident reporting procedure to reflect new timescales	23/10/2017	31/12/2017	
	Update induction and training following the publication of NHS Digital Information Governance Training.	01/01/2018	19/01/2018	
	Develop information leaflet about changes to legislation and ensure this is available in all clinical areas.	22/01/2018	30/03/2018	
	Update SAR policy to include data portability	23/10/2017	31/12/2017	

Task	Detail	date start	due date for completion	complete?
	Posters concerning information rights to be displayed in all public facing departments	22/01/2018	30/03/2018	
	Factsheet for opt-out	06/11/2017	19/01/2018	
	Write staff privacy notice - must include the right to be forgotten.	02/10/2017	31/12/2017	
	Consult with staff about privacy notice	04/12/2017	31/03/2018	
	Develop right to be forgotten process	02/10/2017	31/12/2017	