UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST
BOARD OF DIRECTORS
THURSDAY 26TH MARCH 2015

Title:	**INFORMATION GOVERNANCE TOOLKIT ASSESSMENT**
Responsible Director:	David Burbridge, Director of Corporate Affairs
Contact:	Rachel Seabright, Information Governance Officer, Ext 13707

Purpose:	To: approve the Trust's Information Governance Framework; inform the Board of Directors of the outcome of the Trust's Information Governance Toolkit Assessment for 2014-2015; and to approve submission of the self-assessed score.	
Confidentiality Level & Reason:	None	
Annual Plan Ref:	Deliver an effective governance and assurance system for regulatory requirements.2.4	
Key Issues Summary:	The Trust has carried out its annual self-assessment against the Information Governance Toolkit. The Information Governance Group has reviewed the final scores for the assessment. The overall result for 2014 - 2015 is 76% with a mark of satisfactory. The Trust answered all 45 requirements and achieved level 2 or above for all requirements.	
Recommendations:	The Board of Directors is asked to: 1. review and approve the Information Governance Framework; 2. agree that the Trust submits a score of 76% for the 2014 -15 Information Governance Toolkit assessment (Version 12); and 3. authorise the Director of Corporate Affairs to sign and submit the Information Governance Assurance Statement.	
Approved by:	David Burbridge	26TH March 2015

UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST

BOARD OF DIRECTORS
THURDSAY 26TH MARCH 2015

INFORMATION GOVERNANCE TOOLKIT ASSESSMENT

PRESENTED BY THE DIRECTOR OF CORPORATE AFFAIRS

1. Introduction

The purpose of this paper is to ask the Board to review and approve the Trust's Information Governance Framework, inform the Board of Directors of the outcome of the self-assessment against the Information Governance Toolkit for 2014-2015 (Version 12) and to approve submission of the assessment score to HSCIC.

2. Background to the Information Governance Toolkit

2.1. The Information Governance Toolkit is a self-assessment completed annually by the Trust and submitted to HSCIC at the end of each financial year.

2.2. Version 12 consists of 45 requirements. For each requirement the Trust must self-assess and provide a score. Scoring is on a basis of level 0 up to Level 3, with 3 being the highest.

2.3. The overall score is displayed as a percentage and also marked as satisfactory or unsatisfactory. To achieve a satisfactory mark the Trust is required to achieve level 2 for all 45 requirements.

3. Review of Information Governance Framework

3.1. One of the requirements of the IG Toolkit is that there is an annual review of the Trust's Information Governance Framework. To achieve level 3 for requirement 101 this document must be reviewed by the Board.

3.2. The Framework is attached at Appendix 2.

4. Procedure for self-assessment of scoring of the Information Governance Toolkit

4.1. The scoring for the requirements is completed by the lead for each area and all evidence is uploaded to Health Assure.

4.2. The Information Governance Group, chaired by the Director of Corporate Affairs, has reviewed and agreed the final scores for the assessment.

4.3. In addition, the Trust's Internal Auditors have reviewed elements of the assessment as part of their internal audit programme.

4.4. The Board of Directors is asked to review and approve the completed assessment.

5. Result for the Information Governance Toolkit Assessment for 2014/2015 (Version 12)

5.1. The overall result for 2014 - 2015 (Version 12 Assessment) is 76% with a mark of satisfactory. For a full breakdown please refer to Appendix 1 to this paper.

5.2. The Trust answered all 45 requirements.

5.3. The Trust achieved level 2 or above for all requirements.

6. Comparison with previous year's assessment

6.1. The score for the Information Governance Toolkit assessment for 2013-2014 was 80% with a mark of satisfactory compared to a score of 76% this year. As an updated version of the Toolkit is produced each year, it is difficult to make a reliable comparison with scores from previous assessments. The evidence required to achieve the attainment levels can vary year on year. Furthermore, due to capacity issues and priorities in the relevant departments, for some of the requirements it has been necessary to reduce the level from a 2 to a 3 to take into account business and activity requirements.

6.2. Comparison of number of requirements at each level

Assessment	Stage	Level 0	Level 1	Level 2	Level 3	Total Requirements	Overall Score	Current Grade
Version 11 (2013 – 14)	Published	0	0	26	19	45	80%	Satisfactory
Version 12 (2014 – 15)	Current	0	0	32	13	45	76%	Satisfactory

7. Comparison of previous scores for Information Governance Toolkit Assessments

7.1. Past scores for the Trust:

Year of IG assessment	Score
Version 12 2014-15	76%
Version 11 2013-14	80%
Version 10 2012-13	80%
Version 9 2011-12	77%
Version 8 2010-11	77%
Version 7 2009-10	80%
Version 6 2008-09	79%
Version 5 2007-08	81%

8. Information Governance Assurance Statement

8.1. All organisations submitting an IG Toolkit assessment are required to accept the Information Governance Assurance Statement. This happens at the point of submission.

8.2. The full statement can be viewed at Appendix 3.

9. Recommendations

The Board of Directors is asked to:

9.1. review and approve the Information Governance Framework;

9.2. agree that the Trust submits a score of 76% for the 2014 -15 Information Governance Toolkit assessment (Version 12); and

9.3. authorise the Director of Corporate Affairs to sign and submit the Information Governance Assurance Statement.

David Burbridge
Director of Corporate Affairs **26th March 2015**

Appendix 1

IG Toolkit Completed Assessment

Version 12 (2014-2015) Assessment Requirements List

Req No	Description	Status	Attainment Level
12-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	Confirmed Complete	Level 3
12-105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	Confirmed Complete	Level 3
12-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	Confirmed Complete	Level 2
12-111	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 2
12-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	Confirmed Complete	Level 3
12-200	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
12-201	Staff are provided with clear guidance on keeping personal information secure, on respecting the confidentiality of service users, and on the duty to share information for care purposes	Confirmed Complete	Level 2
12-202	Personal information is shared for care but is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected	Confirmed Complete	Level 2
12-203	Individuals are informed about the proposed uses of their personal information	Confirmed Complete	Level 2
12-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	Confirmed Complete	Level 3
12-206	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	Confirmed Complete	Level 2
12-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	Confirmed Complete	Level 2
12-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	Confirmed Complete	Level 2
12-210	All new processes, services, information systems, and other relevant information assets are developed and	Confirmed Complete	Level 3

	implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements		
12-300	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
12-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	Confirmed Complete	Level 2
12-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	Confirmed Complete	Level 2
12-303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority	Confirmed Complete	Level 3
12-304	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 2
12-305	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 2
12-307	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
12-308	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 2
12-309	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 2
12-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	Confirmed Complete	Level 2
12-311	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
12-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Confirmed Complete	Level 2
12-314	Policy and procedures ensure that mobile computing and teleworking are secure	Confirmed Complete	Level 2
12-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	Confirmed Complete	Level 2
12-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	Confirmed Complete	Level 2
12-400	The Information Governance agenda is supported by adequate information quality and records management	Confirmed Complete	Level 2

	skills, knowledge and experience		
12-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	Confirmed Complete	Level 2
12-402	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 2
12-404	A multi-professional audit of clinical records across all specialties has been undertaken	Confirmed Complete	Level 2
12-406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records	Confirmed Complete	Level 3
12-501	National data definitions, standards, values and validation programmes are incorporated within key systems and local documentation is updated as standards develop	Confirmed Complete	Level 2
12-502	External data quality reports are used for monitoring and improving data quality	Confirmed Complete	Level 2
12-504	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
12-505	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
12-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place	Confirmed Complete	Level 2
12-507	The Completeness and Validity check for data has been completed and passed	Confirmed Complete	Level 3
12-508	Clinical/care staff are involved in validating information derived from the recording of clinical/care activity	Confirmed Complete	Level 2
12-510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national clinical coding standards	Confirmed Complete	Level 2
12-601	Documented and implemented procedures are in place for the effective management of corporate records	Confirmed Complete	Level 2
12-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	Confirmed Complete	Level 2
12-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken	Confirmed Complete	Level 2

Appendix 2

IG Management Framework 2014-2015

Heading	Requirement	Notes
Senior Roles	Senior Information Risk Owner (SIRO) - Director of Corporate Affairs Caldicott Guardian – Medical Director Deputy Director for Corporate Affairs, Legal & Risk IG Lead - Senior Manager Information Governance	These roles should be at Board or the most senior leadership team level. The IG lead and the SIRO may be the same individual but the Caldicott Guardian should be distinct from both of the others and advisory rather than accountable.
Key Policies and procedures	IG Policy (Over-arching policy) Data Protection and Confidentiality Policy Information Security Policy Records Management and Information Lifecycle Policy Freedom of Information Policy Access Control Policy Acceptable Use Policy E-mail Policy	Policies set out scope and intent. The over-arching IG policy should reference the three supporting confidentiality, security and records management policies and might be where the organisation's intended IG Management Framework is documented. Polices are approved by the Trust Policy Review Group in line with the Controlled Documents Policy and Procedure. Polices are communicated as set out in the Controlled Documents Policy and Procedure and made

	Information Security Policy	available on the Trusts intranet site
Key Governance Bodies	Information Governance Group (See Terms of Reference) Director of Corporate Affairs Governance Group	A group, or groups, with appropriate authority should have responsibility for the IG agenda. This might be one or more standalone groups or be part of an Integrated Governance Board or Risk Management group.
Resources	Senior Information Risk Owner (SIRO) - Director of Corporate Affairs Caldicott Guardian – Medical Director Deputy Director for Corporate Affairs, Legal & Risk Senior Manager Information Governance Information Governance Officer Senior Manager Corporate Affairs Informatics Programme Managers Health Records Services Manager IT Security & Compliance Manager	The key staff involved in the IG agenda below those at Board or most senior levels should be identified with a description of their roles and responsibilities. This may include an IG officer, Data Protection Officer, Information Security Officer, Freedom of Information manager, Corporate and Clinical Governance leads or Data quality leads. Any dedicated budgets and high level plans for expenditure in-year should also be identified, including outsourcing to external resources or contractors.

	Information Asset Owners	
Governance Framework	Full details of the Information Governance Framework is included in the Information Governance Policy. The Trust has in place Information Asset Registers. The Trust completes data mapping for flows of personal data. Confidentiality clauses are included in staff contracts of employment. Staff are made aware of their responsibilities through mandatory IG training	This should include staff contracts, contracts with third parties, Information Asset Owner arrangements, Departmental leads on aspects of IG etc.
Training & Guidance	Training for all staff – IG training is mandatory for staff through face to face sessions or via completion of the IG Training Tool All new starters are required to complete Corporate trust induction which includes training in Information Governance. Training for specialist	Staff need clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. The approach to ensuring that all staff receive training appropriate to their roles should be detailed.

	IG roles, e.g. Senior Manager Information Governance, SIRO and IAO's is completed via the relevant modules on the IG Training Tool or specific training sessions Policies and guidance, as detailed above are available to staff via the intranet.	
Contracts of employments	All staff sign contracts of employment which include clauses in confidentiality. All staff are required to comply with Trust polices and national guidance such as DoH Code of Practice on Confidentiality	
Incident Management	All IG incidents are reported via Risk Management and staff are made aware of this via training. IG incidents are managed according to Trust policy and in line with the Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents V2	Clear guidance on incident management procedures should be documented and staff should be made aware of their existence, where to find them and how to implement them.

Appendix 3

Information Governance Assurance Statement

As of 16th September 2009, all organisations submitting an IG Toolkit assessment are required to accept the following Information Governance Assurance Statement. This happens at the point of submission (i.e. when you click the "Submit" button).

The IG Assurance Statement is binding on your organisation and acceptance should be authorised by an appropriate senior individual in the same way as the IG Toolkit assessment itself. The IG Assurance Statement can be printed (using the "Print" button below) prior to acceptance in order to facilitate consideration by authorising individuals.

Information Governance Assurance Statement for Organisations that use, or plan to use HSCIC Services

Version 4, 10/06/2014

1. All organisations that have either direct or indirect access to HSCIC services[1], including N3, must complete an annual Information Governance Toolkit Assessment and agree to the following additional terms and conditions. Where the Information Governance Toolkit requirements are not met to an appropriate standard (minimum level 2), an action plan for making the necessary improvements must be agreed with the HSCIC External Information Governance team or with an alternative body designated by the Department of Health (e.g. a commissioning organisation).
2. All organisations providing indirect access[2] to HSCIC services for other organisations (approved N3 link recipients), are required to provide the Department of Health, on request, with details of all organisations that have been permitted access, the business justification and the controls applied, and must maintain a local log of organisations to which they have allowed access to N3. This log should be reviewed regularly by the organisation and unnecessary access rights removed. The Department of Health or an alternative body designated by the Department of Health may request sight of these logs in order to facilitate or aid audit or investigations.
3. The approved N3 link recipient is responsible for their compliance with IG policies and procedures and may request authorisation by the Department of Health to monitor and enforce the compliance and conduct of subsidiary connected organisations and suppliers to ensure that all key information governance requirements are met.
4. The use of HSCIC Services should be conducted to support NHS business activities that contribute to the care of patients. Usage of individual services must be conducted inline with those individual services requirements and acceptable use policies. The use of HSCIC provided infrastructure or services for unauthorised advertising or other non-healthcare related activity is expressly forbidden.
5. All threats or security events affecting or potentially affecting the security of HSCIC provided infrastructure or services must be immediately reported via

the HSCIC incident reporting arrangements or via local security incident procedures where applicable.

6. All infrastructure and connections to other systems and networks which are not covered by an approved Information Governance Toolkit Assessment and agreement to this IG Assurance Statement must be segregated or isolated from IGT covered infrastructure and connections such that IGT covered infrastructure and connections, or HSCIC Services are not put at risk. A Logical Connection Architecture diagram must be maintained by network managers in accordance with HSCIC guidance and must be provided for Department of Health review on request.
7. Organisations with access to HSCIC Services shall ensure that they meet the requirements of the Department of Health policy on person identifiable data leaving England, or being viewed from overseas. A copy of the Information Governance Offshore Support Requirements applicable to those accessing HSCIC Services is available on request or can be downloaded from http://systems.hscic.gov.uk/infogov/igsoc/links/index_html. The agreement of the Department to this limited support or exceptionally to more extensive processing must be explicitly obtained.
8. Where another network is connected to N3, only services that have been previously considered and approved by the Department of Health as appropriate for that network are permissible. Requests for new or changed services must be provided to the Department for consideration.
9. Organisations may not create or establish any onward connections to the N3 Network or HSCIC provided services from systems and networks which are not covered by an approved Information Governance Toolkit Assessment and agreement to this IG Assurance Statement.
10. The approved organisation shall allow the Department of Health, or its representatives, to carry out ad-hoc on-site audits, and to review any/all evidence that supports the Information Governance Toolkit Assessment, as necessary to confirm compliance with these terms and conditions and with the standards set out in the Information Governance Toolkit.

Information Governance Assurance Statement

I confirm that I have read, understood and agree to comply with the additional terms and conditions that apply to organisations that have access to HSCIC services and acknowledge that failure to maintain compliance may result in the withdrawal of HSCIC services.

---

[1] HSCIC Services include the N3 network and other applications or services provided by HSCIC, e.g. the NHS Spine Service, NHSmail, Choose and Book (and in future the NHS e-Referral Service).

[2] Access to the N3 network or HSCIC Services via another organisation or gateway