UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST

BOARD OF DIRECTORS

29 MARCH 2018

Title:	**INFORMATION GOVERNANCE TOOLKIT ASSESSMENT**
Responsible Director:	David Burbridge, Director of Corporate Affairs
Contact:	Berit Reglar, Deputy Foundation Secretary, Ext 14324

Purpose:	To inform the Board of Directors of the changes to the Information Governance Toolkit and the Trust's self-assessed score for the Information Governance Toolkit Assessment for 2017-18.	
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 overall result for 2017 – 2018 is 69% 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 approve the Information Governance Policy; and 2 agree that the Trust submits a score of 69% for the 2017-18 Information Governance Toolkit assessment.	
Approved by:	David Burbridge	March 2018

UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST

BOARD OF DIRECTORS
29 MARCH 2018

INFORMATION GOVERNANCE TOOLKIT ASSESSMENT

PRESENTED BY THE DIRECTOR OF CORPORATE AFFAIRS

1. Introduction

The purpose of this paper is to:

1.1. inform the Board of Directors of the Trust's score for the Information Governance Toolkit Assessment for 2017-18 (Version 14.1);

1.2. ask the Board to approve the assessment prior to its final submission to HSCIC Services (NHS Digital).

2. Background to the Information Governance Toolkit (IGT)

2.1. Since 16 September 2009 it is a requirement for all NHS Trusts to complete an Information Governance Toolkit (IGT) self-assessment annually and to submit the same to HSCIC at the end of each financial year. From 1 April 2018 this will be superseded by the Data Security and Protection (DSP) Toolkit Requirements, issued by NHS Digital.

2.2. Since 2015/16 there is a mandatory requirement to have as a minimum 8 standards of the IG Toolkit assessment audited by the Trust's Internal Auditors. The Internal Audit IGT report resulted in 'significant assurance with minor improvements opportunities' and was presented to the Audit Committee at the March meeting.

2.3. Version 14.1 of the IGT 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.

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

3. Result for the Information Governance Toolkit Assessment for 2017/2018 (Version 14)

3.1. The overall result for 2017 - 2018 (Version 14.1 Assessment) is 69% with a mark of 'satisfactory' compared to 70% for 2016 – 2017 (see also table 1 and 2 below). The Trust answered all 45 requirements. The

Trust achieved level 2 for all requirements. For a full breakdown please refer to Appendix 1.

3.2. There has been a slight decrease in the overall score by 1% points. An updated version of the Toolkit is produced each year which renders it difficult to make a reliable comparison with scores from previous assessments. In addition, the evidence required to achieve the attainment levels varies year on year, where level 3 has been achieved previously additional evidence is required to maintain that level, which the Trust may not have. For 2017 - 2018 it was necessary to reduce some requirements relating to IG framework, training and FOI request from level 3 to a level 2 due to the impact of Controlled Document and process alignment with HoEFT.

Table 1: Comparison of number of requirements at each level

Assessment	Stage	L0	L1	L2	L3	Total Requirements	Overall Score	Current Grade
Version 11 (2013 – 14)	Published	0	0	26	19	45	80%	Satisfactory
Version 12 (2014 – 15)	Published	0	0	32	13	45	76%	Satisfactory
Version 13 (2015 – 16)	Published	0	0	37	8	45	72%	Satisfactory
Version 14 (2016 – 17)	Published	0	0	40	5	45	70%	Satisfactory
Version 14.1 (2017 – 18)	Current	0	0	45	0	45	69%	Satisfactory

Table 2: Comparison of previous IGT scores

Year of IG assessment	Score
Version 14.1 2017-18	69%
Version 14 2016-17	70%
Version 13 2015-16	72%
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%
Version 4 2006-07	89%
Version 3 2005-06	92%
Version 2 2004-05	90%
Version 1 2003-04	76%

4. Information Governance Development

The following points are to inform the Board of new developments in respect of Information Governance:

4.1. March 2018 – the new “Data Opt –out” initiative by the National Data Guardian has been made available online, providing a secure way for patients to express their preference(s) about sharing their data for reasons other than their individual care and treatment. Patients are able to access the opt-out online, using a smartphone, tablet or personal computer. The requirement to uphold the national data opt-out will be phased in, with the full roll out across the health and care system by 2020.

4.2. April 2018 - Roll out of IG Toolkit redesign into a new user friendly “Data Security and Protection Toolkit” (DSPT) which will be compliant with the 2016 EU General Data Protection Regulation (GDPR). The Trust will benefit from an accessible dashboard enabling to track progress in meeting the 10 Data Security Standards. Further details are available on the NHS Digital website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/675420/17-18_statement_of_requirements_Branded_template_final_22_11_18-1.pdf

4.3. May 2018 – the Data Protection Bill is expected to be approved as the UK Data Protection Act 2018, as amended by the GDPR, which comes into force on 25 May 2018.

4.4. May 2018 – the Network and Information System (NIS) Directive is to be implemented into UK law by 9 May 2018. Network and information system security incidents (incidents) will have to be reported to the Secretary of State for Health (as Competent Authority) without undue delay and at the latest within 72 hours of 72 hours. When identifying appropriate and proportionate technical and organisational measures, a risk based approach will need to be taken, considering the physical and environmental security, security of supplies, access controls, and the systematic management of network and information systems (which are further defined in Art 3 of the Implementation Regs). A breach of a reportable incident may result in a maximum fine of £17m (the UK does not propose to a have two or three tier approach, but just one maximum fine). There is recognition of the double-jeopardy argument in that certain incidents might be fined under the NIS Directive and GDPR

5. Information Governance Assurance Statement

5.1. All organisations submitting an IG Toolkit assessment are required to accept the Information Governance Assurance Statement. Acceptance automatically occurs at the point of submission.

5.2. The full statement can be viewed at Appendix 2.

6. Recommendations

The Board of Directors is asked to agree that the Trust submits a score of 69% for the 2017 -18 Information Governance Toolkit assessment (Version 14.1).

David Burbridge
Director of Corporate Affairs **March 2018**

Appendix 1 - IG Toolkit Completed Assessment

Version 14.1 (2017 -2018) Assessment Requirements List

INFORMATION GOVERNANCE MANAGEMENT		
14-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	Level 2
14-105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	Level 2
14-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	Level 2
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	Level 2
14-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	Level 2
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	Level 2
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	Level 2
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	Level 2
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	Level 2
14-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	Level 2
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	Level 2
14-207	Where required, protocols governing the routine sharing of	Level 2

	personal information have been agreed with other organisations	
14-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	Level 2
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	Level 2
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	Level 2
14-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	Level 2
14-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	Level 2
14-303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority	Level 2
14-304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use	Level 2
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	Level 2
14-307	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy	Level 2
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	Level 2
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	Level 2
14-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	Level 2

14-311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	Level 2
14-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Level 2
14-314	Policy and procedures ensure that mobile computing and teleworking are secure	Level 2
14-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	Level 2
14-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	Level 2
CLINICAL INFORMATION ASSURANCE		
14-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	Level 2
14-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	Level 2
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	Level 2
14-404	A multi-professional audit of clinical records across all specialties has been undertaken	Level 2
14-406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records	Level 2
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	Level 2
14-502	External data quality reports are used for monitoring and improving data quality	Level 2
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	Level 2
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	Level 2
14-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place	Level 2

14-507	The secondary uses data quality assurance checks have been completed	Level 2
14-508	Clinical/care staff are involved in quality checking information derived from the recording of clinical/care activity	Level 2
14-510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national clinical coding standards	Level 2
CORPORATE INFORMATION ASSURANCE		
14-601	Documented and implemented procedures are in place for the effective management of corporate records	Level 2
14-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	Level 2
14-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken	Level 2

Appendix 2

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