NHS
Ashford and St. Peter's Hospitals
NHS Foundation Trust

TRUST BOARD
29 March 2018

AGENDA ITEM	19.1
TITLE OF PAPER	Information Governance Toolkit V14.1
Confidential	**NO**
Suitable for public access	**YES**

PLEASE DETAIL BELOW THE OTHER SUB-COMMITTEE(S), MEETINGS THIS PAPER HAS BEEN VIEWED

IG Steering Group

STRATEGIC OBJECTIVE(S):

Best outcomes		Compliance with the IGTK
Excellent experience		
Skilled & motivated teams		
Top productivity		Assurance on the integrity of the IGTK submission.

EXECUTIVE SUMMARY	
	The Information Governance Toolkit is a mandatory annual requirement for all NHS organisations. Following internal review of the Trust's evidence uploaded for 45 requirements, the provisional self-assessment for 2017-18 was graded as 'Satisfactory'. The IG Toolkit has been submitted with a score of 72%.
RECOMMENDATION:	The Board is asked to approve the submission of the Trust's Information Governance Toolkit return for 2017-18, and acceptance of the Information Governance Assurance Statement, as detailed within this report.

SPECIFIC ISSUES CHECKLIST:

Quality and safety	Compliance with the IGTK is essential in order to stay connected to N3 and be able to share information with our partner organisations.
Patient impact	
Employee	
Other stakeholder	
Equality & diversity	

Finance	
Legal	
Link to Board Assurance Framework Principle Risk	Assurance to the Board that the information uploaded as evidence to the IGTK is trustworthy and accurate. Failure to meet the standards described in the toolkit may result in legal breaches and non-compliance with NHS regulations. Additionally, failure to meet a 'Satisfactory' grading against the toolkit itself may jeopardise the Trust's access to national NHS services provided by NHS Digital, and the Trust's ability to share information with other healthcare organisations.
AUTHOR	Laura Ellis-Philip, Associate Director of Informatics
PRESENTED BY	Simon Marshall, Director of Finance and Information
DATE	26 March 2013
BOARD ACTION	Assurance

NHS
Ashford and St. Peter's Hospitals
NHS Foundation Trust

TRUST BOARD
29 Mar 18

Information Governance Toolkit V14.1

Background

Self-assessment using the Information Governance Toolkit ("**IGT**") is an annual requirement for all organisations processing NHS patient data, mandated by the Department of Health. The IGT represents evidence-based assurance of compliance with the legal and regulatory requirements on NHS bodies in regard of information security and risk management, confidentiality and data protection, and records management and information quality.

For acute trusts, the 2017-18 version of the IGT (known as V14.1) consists of 45 requirements, shown in Appendix 1, each of which are divided into three levels of compliance. A minimum of Level 2 is required on each element in order to attain an overall 'Satisfactory' grading. A percentage score is also calculated against the highest possible score of Level 3 for each element, but it does not contribute to the grading of 'Satisfactory' or 'Not Satisfactory'.

Self-Assessment

The Trust's submission is completed, with the Trust achieving a 'Satisfactory' score. The declaration is shown below in purple, with previous years' results for comparison:

Assessment	Stage	Level 0	Level 1	Level 2	Level 3	Score	Grade
V14.1 (2017/18)	Published	0	0	37	8	72%	Satisfactory
V14 (2016/17)	Published	0	0	38	7	71%	Satisfactory
V13 (2015/16)	Target	0	1	21	23	82%	Not Satisfactory
V12 (2014/15)	Published	0	0	19	26	85%	Satisfactory
V11 (2013/14)	Published	0	0	40	5	70%	Satisfactory
V10 (2012/13)	Published	0	0	38	7	71%	Satisfactory
V9 (2011/12)	Published	0	3	35	7	69%	Not Satisfactory
V8 (2010/11)	Published	0	1	37	7	71%	Not Satisfactory

The Trust has declared eight requirements at the maximum Level 3 which represents an increase of one on last year's submission. This number of Level 3s continues to reflect the significant changes made to version 13 of the IG Toolkit where additional work is required in order achieve a level 3 score with no incentive for doing so.

There is a requirement to achieve a compliance level of 95% of staff trained in Information Governance. In 2016 the online training tool was decommissioned and organisations were permitted to count two years' worth of training as compliant. The new online training tool is now available and the IT Training team have also increased the number of training sessions available. All new staff complete IG training at induction.

The ESR compliance statistics are unreliable as they change on a daily basis and seem to run about three months in arrears – this is largely due to the reliance on the staff member to inform their line manager that they have completed the training, and then the line manager has to update ESR. In addition, we can see that many staff wait until their period of compliance has ended and then book onto a course within the next 12 weeks.

We find that there are staff groups such as junior doctors, locums and volunteers, whose training compliance is not recorded using ESR in a standardised fashion. Bank staff records are also not routinely updated to reflect training compliance.

With the above in mind, we have examined the training statistics and identified staff whose ESR records have no evidence of ever having completed IG training. Of permanent staff, these number 2%. A further 1.6% have compliance dating back to a point between 2013 and 2015. We have sent these staff the IG training presentation for their immediate perusal, and a reminder of their IG responsibilities and a requirement to access training without delay.

There are a number of staff showing compliance in 2016, 2017 and early 2018. We have deemed these staff to be compliant on the basis that the online training tool was not available until July 2017 and does not automatically update ESR in the way that it used to. We also feel that it takes time for the message to reach staff that they must resume accessing IG training annually, but we can see from the numbers attending recent training that this message is now having an effect. The IT Training team are

Audit

This is the final year of the IG Toolkit in its current form, with a completely new version ready for release in preparation for next year's submission. With this in mind, and because an annual audit is not a pre-requisite, the Senior Information Risk Owner (DoF&I) agreed with the recommendation from the Information Governance Steering Group not to perform an audit for this year.

Next year

The new toolkit is named the **Data Security and Protection Toolkit**, and is understood to provide good guidance from a General Data Protection Regulations (GDPR) and cyber security perspective. It is also worth noting that certain sections of it will come under CQC scrutiny and compliance with them will form part of the CQC assessment.

Information Governance Assurance Statement

Since Sep 2009, all organisations submitting an IGT assessment are required to accept the national Information Governance Assurance Statement as part of the submission. The statement sets out the Department of Health's requirements for organisations accessing NHS Digital's services.

The full statement is attached verbatim at Appendix 2, and has no material changes from previous years' versions accepted by the Trust.

Conclusion

The Trust considers its information governance practices represent robust compliance to the IGT overall which provides assurance against legal and NHS requirements.

The Board is asked to approve the self-assessment as determined by the Trust's internal review process, and the submission to the Department of Health including acceptance of the associated Information Governance Assurance Statement.

NHS
Ashford and St. Peter's Hospitals
NHS Foundation Trust

Appendix 1

Information Governance Toolkit V14 requirements and target declarations

Req No	Description	Target
Information Governance Management		
13-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	**3**
13-105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	**3**
13-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	**2**
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	**2**
13-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	**2**
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	**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	**2**
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	**2**
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	**2**
13-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	**2**
13-206	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	**3**
13-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	**2**
13-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	**2**
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	**2**
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	**3**
13-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	**2**
13-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	**2**
13-303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority	**2**
13-304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use	**2**
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	**2**
13-307	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy	**2**
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	**2**
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	**2**
13-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	**2**
13-311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	**2**
13-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	**2**
13-314	Policy and procedures ensure that mobile computing and teleworking are secure	**2**
13-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	**3**
13-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	**2**
Clinical Information Assurance		
13-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	**2**
13-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	**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	**2**
13-404	A multi-professional audit of clinical records across all specialties has been undertaken	**2**
13-406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records	**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	**2**
13-502	External data quality reports are used for monitoring and improving data quality	**2**
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	**2**
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	**2**
13-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place	**2**
13-507	The secondary uses data quality assurance checks have been completed	**2**
13-508	Clinical/care staff are involved in validating information derived from the recording of clinical/care activity	**2**
13-510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national clinical coding standards	**2**
Corporate Information Assurance		
13-601	Documented and implemented procedures are in place for the effective management of corporate records	**2**
13-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	**2**
13-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken	**2**

NHS
Ashford and St. Peter's Hospitals
NHS Foundation Trust

Appendix 2

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