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

TRUST BOARD
29th March 2012

TITLE	**Information Governance (IG) Toolkit**
EXECUTIVE SUMMARY	The security of data and information is fundamental to the delivery of healthcare and is a major challenge for NHS organisations given the increasing need to maximise the availability and sharing of information across care settings. Since 2008, concerns about public sector data protection have resulted in the Cabinet Office mandating a range of standards for managing information risk, an important element of information governance. These standards are reflected within the NHS Information Governance Toolkit. All NHS Trusts are required to self-assess against a diverse range of standards and to provide evidence that demonstrates compliance with these standards. Trusts are expected to achieve Level 2 compliance across all requirements. Trust Board is asked to approve the self-assessment and to submitting the IG Toolkit by 31st March 2012.
BOARD ASSURANCE (RISK)/ IMPLICATIONS	Failure to maintain the highest standards of information governance could lead to poor patient care and non compliance with NHS standards and legislation
STAKEHOLDER/ PATIENT IMPACT AND VIEWS	None known.
EQUALITY AND DIVERSITY ISSUES	None known.
LEGAL ISSUES	None known
The Trust Board is asked to:	To approve the self-assessment and submission of the 2011-12 IG Toolkit
Submitted by:	Donna M Jarrett, Associate Director Health Informatics/IG Lead for John Headley, Director of Finance & Information/Senior Information Risk Owner (SIRO)
Date:	22nd March 2012
Decision:	To approve

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

TRUST BOARD
29th March 2012

Information Governance (IG) Toolkit

1. Introduction

The purpose of this paper is to seek Trust Board approval to the self-assessment of compliance and to the submission of the 2011-12 Information Governance Toolkit by 31st March 2012.

2. Background

The security of data and information is fundamental to the delivery of healthcare and is a major challenge for NHS organisations given the increasing need to maximise the availability and sharing of information across care settings.

Since 2008, concerns about public sector data protection have resulted in the Cabinet Office mandating a range of standards for managing information risk, an important element of information governance. These standards are reflected within the NHS Information Governance Toolkit.

All NHS Trusts are required to self-assess against a diverse range of standards and to provide evidence that demonstrates compliance with these standards. There are 45 requirements. Trusts are expected to achieve Level 2 compliance across all requirements.

3. Self-Assessment of Compliance

Attached as Appendix 1 is a summary of the 45 requirements that the Trust has to demonstrate its compliance. Against each requirement is an assessment of compliance.

Out of 45 requirements:

5 requirements have achieved Level 3
37 requirements have achieved Level 2
3 requirements have achieved Level 1

Attention is drawn to the following requirements:

9-112 IG Training
9-324 Pseudonymisation
9-604 Corporate Records

<u>9-112 IG Training</u>

Last year the Trust achieved 96% of staff trained. This achievement was helped by the training target being extended to 30th June 2011. This year the attainment is 56%. Previous advice has been that staff trained between 1 April and 30 June could not be included in the calculation. At the time of writing, Internal Audit has confirmed that this position has now changed and a recalculation of trained staff now needs to be done. An update on the numbers trained will be provided at the Trust Board meeting.

9-324 Pseudonymisation and 9-604 Corporate Records

The Trust has an action plan in place and this requirement will be compliant to Level 2 by 30th June 2012.

Internal Audit has reviewed the self-assessment and is in agreement with the compliance achieved; the Trust is not an outlier and is performing well compared to other Trusts.

4. Approval

The Trust Board is asked to approve the self-assessment of compliance and to submitting the IG Toolkit by 31st March 2012.

Version 9 (2011-2012) Assessment

Requirements List

Req No	Description	Status	Attainment Level
Information Governance Management			
9-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	Reviewed And Updated	Level 2
9-105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	Reviewed And Updated	Level 2
9-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	Reviewed And Updated	Level 2
9-111	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation	Reviewed And Updated	Level 2
9-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	Reviewed And Updated	Level 2
Confidentiality and Data Protection Assurance			
9-200	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs	Reviewed And Updated	Level 2
9-201	Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users	Reviewed And Updated	Level 3
9-202	Personal information 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	Reviewed And Updated	Level 2
9-203	Individuals are informed about the proposed uses of their personal information	Reviewed And Updated	Level 2
9-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	Reviewed And Updated	Level 3
9-206	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	Reviewed And Updated	Level 3
9-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	Reviewed And Updated	Level 2
9-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	Reviewed And Updated	Level 2

9-210	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	Reviewed And Updated	Level 3
Information Security Assurance			
9-300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	Reviewed And Updated	Level 2
9-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	Reviewed And Updated	Level 2
9-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	Reviewed And Updated	Level 2
9-303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority	Reviewed And Updated	Level 2
9-304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use	Reviewed And Updated	Level 2
9-305	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	Reviewed And Updated	Level 2
9-307	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy	Reviewed And Updated	Level 2
9-308	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	Reviewed And Updated	Level 2
9-309	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	Reviewed And Updated	Level 2
9-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	Reviewed And Updated	Level 2
9-311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	Reviewed And Updated	Level 2
9-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Reviewed And Updated	Level 2
9-314	Policy and procedures ensure that mobile computing and teleworking are secure	Reviewed And Updated	Level 2
9-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	Reviewed And Updated	Level 2
9-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	Reviewed And Updated	Level 1
Clinical Information Assurance			
9-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	Reviewed And Updated	Level 2

9-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	Reviewed And Updated	Level 2
9-402	Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care	Reviewed And Updated	Level 2
9-404	A multi-professional audit of clinical records across all specialties has been undertaken	Reviewed And Updated	Level 2
9-406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records	Reviewed And Updated	Level 2
Secondary Use Assurance			
9-501	National data definitions, standards, values and validation programmes are incorporated within key systems and local documentation is updated as standards develop	Reviewed And Updated	Level 2
9-502	External data quality reports are used for monitoring and improving data quality	Reviewed And Updated	Level 2
9-504	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	Reviewed And Updated	Level 2
9-505	A robust programme of internal and external data quality/clinical coding audit in line with the requirements of the Audit Commission and NHS Connecting for Health is in place	Reviewed And Updated	Level 2
9-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place	Reviewed And Updated	Level 2
9-507	The Completeness and Validity check for data has been completed and passed	Reviewed And Updated	Level 2
9-508	Clinical/care staff are involved in validating information derived from the recording of clinical/care activity	Reviewed	Level 2
9-510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national standards	Reviewed And Updated	Level 3
Corporate Information Assurance			
9-601	Documented and implemented procedures are in place for the effective management of corporate records	Reviewed And Updated	Level 2
9-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	Reviewed And Updated	Level 2
9-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken	Reviewed And Updated	Level 1