Appendix 2

Information Governance Toolkit Version 12 Implementation Plan

Current Position as at 31 March 2015

Req No	Description	Status	Current Attainment Level
Information Governance Management			
12-130	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda.	Compliant	Level 3
12-131	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans.	Compliant	Level 3
12-132	Formal contractual arrangements that include compliance with information governance requirements are in place with all contractors and support organisations.	Compliant	Level 2
12-133	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation.	Compliant	Level 2
12-134	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained.	Compliant	Level 2
Confidentiality and Data Protection Assurance			
12-340	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs.	Compliant	Level 3
12-231	Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users.	Compliant	Level 2
12-232	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.	Compliant	Level 2
12-234	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data.	Compliant	Level 2

12-235	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	Compliant	Level 2
12-236	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines.	Compliant	Level 2
12-237	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.	Compliant	Level 2
12-250	Individuals are informed about the proposed uses of their personal information.	Compliant	Level 2
Information Security Assurance			
12-340	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs.	Compliant	Level 2
12-341	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed.	Compliant	Level 2
12-342	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority.	Compliant	Level 2
12-343	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use.	Compliant	Level 2
12-344	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.	Compliant	Level 2
12-345	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy	Compliant	Level 2
12-346	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.	Compliant	Level 2
12-347	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely.	Compliant	Level 2
12-348	Policy and procedures ensure that mobile computing and teleworking are secure.	Compliant	Level 2

12-349	There are documented incident management and reporting procedures	Compliant	Level 2
12-350	All transfers of hardcopy and digital personal and sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers	Compliant	Level 2
12-351	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures.	Compliant	Level 2
12-352	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate.	Compliant	Level 2
Clinical Information Assurance			
12-420	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience.	Compliant	Level 2
12-421	There is a consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	Compliant	Level 2