West Hertfordshire Hospitals NHS

NHS Trust

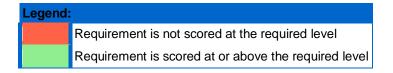## Appendix 1 – Information Governance End of Year Submission

WEST HERTFORDSHIRE HOSPITALS NHS TRUST as at 31/03/2012

Legend:

	Requirement is not scored at the required level
	Requirement is scored at or above the required level

Requirement	Description	Baseline	Update	Final
101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	3	3	3
105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	3	3	3
110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	2	2	2
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	3	3
112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	1	1	1
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	3	3
201	Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users	2	2	2
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	2	2	2
203	Individuals are informed about the proposed uses of their personal information	2	2	2
205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	3	3	3
206	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	2	2	2

207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	2	2	2
209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	2	3	3
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	2	2
300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	3	3	3
301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	2	2	2
302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	3	3	3
303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority	2	2	2
304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use	2	2	2
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	2	2
307	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy	3	3	3
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	3	3
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	2	2
310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	2	2	2
311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	2	2	2
313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	2	2	2
314	Policy and procedures ensure that mobile computing and teleworking are secure	2	3	3
323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical	2	2	2

		measures			
	324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	2	2	2
	400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	3	3	3
	401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	2	2	2
	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	2	2
	404	A multi-professional audit of clinical records across all specialties has been undertaken	2	2	2
	406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records	3	3	3
	501	National data definitions, standards, values and validation programmes are incorporated within key systems and local documentation is updated as standards develop	2	2	2
	502	External data quality reports are used for monitoring and improving data quality	2	2	2
	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**	**3**	**3**
	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	3	3	3
	506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place	2	2	2
	507	The Completeness and Validity check for data has been completed and passed	2	2	2
	508	Clinical/care staff are involved in validating information derived from the recording of clinical/care activity	2	2	2
	510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national standards	3	3	3
	601	Documented and implemented procedures are in place for the effective management of corporate records	2	2	2
	603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	2	3	3
	604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken	2	2	2
Total (%)			**74%**	**78%**	**78%**