Version 14 (2016-2017) Assessment

Requirements List

Req No	Description	Attainment Level
Information Governance Management		
14-114	Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff	Level 3
14-115	There is an information governance policy that addresses the overall requirements of information governance	Level 3
14-116	All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities	Level 3
14-117	All staff members are provided with appropriate training on information governance requirements	Level 3
Confidentiality and Data Protection Assurance		
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 3
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 3
14-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	Not Relevant
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 3
14-211	All transfers of personal and sensitive information are conducted in a secure and confidential manner	Level 3
Information Security Assurance		
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 3
14-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Level 3
14-314	Policy and procedures ensure that mobile computing and teleworking are secure	Level 3
14-316	There is an information asset register that includes all key information, software, hardware and services	Level 3
14-317	Unauthorised access to the premises, equipment, records and other assets is prevented	Level 3
14-319	There are documented plans and procedures to support business continuity in the event of power failures, system failures, natural disasters and other disruptions	Level 3
14-320	There are documented incident management and reporting procedures	Level 3
14-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	Level 3