IG Toolkit V14 to V14.1 Requirement Updates

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	Yes this is included in NDG Standard 1 Assertion 1.1 There is senior ownership of data security and protection within the organisation.	√	√	√	√	√	√	√				√	√									√	√	√	√
14.1-105	There are approved and comprehensive IG Policies with associated Strategies and/or improvement plans	Yes this is included in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to	√	√	√	√	√	√	√				√	√									√	√	√	√
14.1-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	This is covered over a range of Standard in NDG 10, Assertion 10.1 The organisation can name its suppliers, the products and services they deliver and the contract durations. 10.2 Basic due diligence has been undertaken against each supplier according to ICO and NHS Digital guidance. 10.3 All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented. 10.4 All instances where organisations cannot comply with the NDG Standards because of supplier-related issues are recorded and flagged to NHS Digital. 10.5 Where a supplier processes or has access to personal confidential information they have completed CareCERT Assurance.	√	√	√	√	√	√	√				√	√									√	√	√	√
14.1-111	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation	Yes in NDG Standard 2 Assertion 2.3 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.	√	√	√	√	√	√	√				√	√									√	√	√	√
14.1-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	Yes in NDG Standard 3 Assertions 3.1 There has been an assessment of data security and protection training needs across the organisation. 3.2 Staff receive suitable data security and protection training. 3.3 Staff pass the data security and protection mandatory test. 3.4 Staff with specialist roles receive data security and protection training suitable to their role. 3.5 Leaders and board members receive suitable data protection and security training.	√	√	√	√	√	√	√				√	√									√	√	√	√
14.1-114.1	Responsibility for Information Governance has been assigned to an appropriate member or members of staff	Yes in NDG Standard 1 Assertion 1.1 There is senior ownership of data security and protection within the organisation.													√	√	√	√	√	√	√					
14.1-115	There is an Information Governance Policy that addresses the overall requirements of information governance	NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.													√	√	√	√	√	√	√					

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-116	All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities	This is covered over a range of Standard in NDG 10, 10.1 The organisation can name its suppliers, the products and services they deliver and the contract durations. 10.2 Basic due diligence has been undertaken against each supplier according to ICO and NHS Digital guidance. 10.3 All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented. 10.4 All instances where organisations cannot comply with the NDG Standards because of supplier-related issues are recorded and flagged to NHS Digital. 10.5 Where a supplier processes or has access to personal confidential information they have completed CareCERT Assurance.													√	√	√	√	√	√	√				
14.1-117	All staff members are provided with appropriate training on information governance requirements	Yes in NDG Standard 3 Assertions 3.1 There has been an assessment of data security and protection training needs across the organisation. 3.2 Staff receive suitable data security and protection training. 3.3 Staff pass the data security and protection mandatory test. 3.4 Staff with specialist roles receive data security and protection training suitable to their role. 3.5 Leaders and board members receive suitable data protection and security training.													√	√	√	√	√	√	√				
14.1-120	Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff	Yes in NDG Standard 1 Assertion 1.1 There is senior ownership of data security and protection within the organisation.													√										
14.1-121	There is an information governance policy that addresses the overall requirements of information governance	NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.													√										

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-122	All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities.	Yes in NDG Standard 2 Assertion 2.3 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards. This is also covered over a range of Standard in NDG 10, 10.1 The organisation can name its suppliers, the products and services they deliver and the contract durations. 10.2 Basic due diligence has been undertaken against each supplier according to ICO and NHS Digital guidance. 10.3 All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented. 10.4 All instances where organisations cannot comply with the NDG Standards because of supplier-related issues are recorded and flagged to NHS Digital. 10.5 Where a supplier processes or has access to personal confidential information they have completed CareCERT Assurance.												√												
14.1-123	All staff members are provided with appropriate training on information governance requirements.	Yes in NDG Standard 3 Assertions 3.1 There has been an assessment of data security and protection training needs across the organisation. 3.2 Staff receive suitable data security and protection training. 3.3 Staff pass the data security and protection mandatory test. 3.4 Staff with specialist roles receive data security and protection training suitable to their role. 3.5 Leaders and board members receive suitable data protection and security training.												√												
14.1-130	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	Yes this is included in NDG Standard 1 Assertion 1.1 There is senior ownership of data security and protection within the organisation.									√															
14.1-131	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	Yes this is included in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.									√															

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-132	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	This is covered over a range of Standard in NDG 10, Assertion 10 10.1 The organisation can name its suppliers, the products and services they deliver and the contract durations. 10.2 Basic due diligence has been undertaken against each supplier according to ICO and NHS Digital guidance. 10.3 All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented. 10.4 All instances where organisations cannot comply with the NDG Standards because of supplier-related issues are recorded and flagged to NHS Digital. 10.5 Where a supplier processes or has access to personal confidential information they have completed CareCERT Assurance.									√																
14.1-133	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation	Yes in NDG Standard 2 Assertion 2.3 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.									√															
14.1-134	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	Yes in NDG Standard 3 Assertions 3.1 There has been an assessment of data security and protection training needs across the organisation. 3.2 Staff receive suitable data security and protection training. 3.3 Staff pass the data security and protection mandatory test. 3.4 Staff with specialist roles receive data security and protection training suitable to their role. 3.5 Leaders and board members receive suitable data protection and security training.									√															
14.1-14.10	Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff	Yes in NDG Standard 1 Assertion 1 1.1 There is senior ownership of data security and protection within the organisation.										√														
14.1-14.11	There is an information governance policy that addresses the overall requirements of information governance	Yes this is included in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.										√														

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-14.12	All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities	Yes in NDG Standard 2 Assertion 2.3 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards. This is also covered over a range of Standard in NDG 10, 10.1 The organisation can name its suppliers, the products and services they deliver and the contract durations. 10.2 Basic due diligence has been undertaken against each supplier according to ICO and NHS Digital guidance. 10.3 All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented. 10.4 All instances where organisations cannot comply with the NDG Standards because of supplier-related issues are recorded and flagged to NHS Digital. 10.5 Where a supplier processes or has access to personal confidential information they have completed CareCERT Assurance.										√														
14.1-14.13	All staff members are provided with appropriate training on information governance requirements	Yes in NDG Standard 3 Assertions 3.1 There has been an assessment of data security and protection training needs across the organisation. 3.2 Staff receive suitable data security and protection training. 3.3 Staff pass the data security and protection mandatory test. 3.4 Staff with specialist roles receive data security and protection training suitable to their role. 3.5 Leaders and board members receive suitable data protection and security training.										√														
14.1-14.14	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	Yes this is included in NDG Standard 1 Assertion 1.1 There is senior ownership of data security and protection within the organisation.								√																
14.1-14.15	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	Yes this is included in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.								√																

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-14.16	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	This is covered over a range od Standard in NDG 10, Assertion 10 10.1 The organisation can name its suppliers, the products and services they deliver and the contract durations. 10.2 Basic due diligence has been undertaken against each supplier according to ICO and NHS Digital guidance. 10.3 All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented. 10.4 All instances where organisations cannot comply with the NDG Standards because of supplier-related issues are recorded and flagged to NHS Digital. 10.5 Where a supplier processes or has access to personal confidential information they have completed CareCERT Assurance.								√																	
14.1-14.17	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation	Yes in NDG Standard 2 Assertion 2.3 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.								√																	
14.1-14.18	The training needs of all staff are assessed in relation to Information Governance requirements and they are all appropriately trained	Yes in NDG Standard 3 Assertion 3.4 Staff with specialist roles receive data security and protection training suitable to their role.								√																	
14.1-200	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs	Yes this is included in NDG Standard 1 Assertion 1.1 There is senior ownership of data security and protection within the organisation.	√	√	√	√	√	√	√				√	√									√	√	√	√
14.1-201	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	Yes this is included in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 1.5 Personal information is used and shared lawfully. This is also covered in NDG Standard 2 Assertion 2.2 Personal Confidential Information is processed/shared legally and securely. 2.3 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.	√	√	√	√	√	√	√				√	√									√	√	√	√

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-201-CSU Variant	Staff are provided with clear guidance on keeping personal information secure, on respecting the confidentiality of service users, and on the duty to share information for care purposes	Yes this is included in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. NDG Standard 1 Assertion 1.5 Personal information is used and shared lawfully. This is also covered in NDG Standard 2 2.2 Personal Confidential Information is processed/shared legally and securely. 2.3 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.				√																				
14.1-202	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	Yes this is included in NDG Standard 1 Assertion 1.3 Individuals' rights are respected and supported (GDPR Art 12-22) 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully.	√	√	√	√	√	√	√				√	√			√					√	√	√	√	√
14.1-203	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	Yes this is included in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. NDG Standard 1 Assertion 1.3 Individuals' rights are respected and supported (GDPR Art 12-22) NDG Standard 1 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4)	√	√	√	√	√	√					√	√		√										
14.1-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	Yes this is covered by NDG Standard 1 Assertion 1.3 Individuals' rights are respected and supported (GDPR Art 12-22)	√	√	√	√	√	√	√				√	√		√							√	√	√	√

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-206	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.	This is covered by NDG Standard 1 Assertions: 4.1 The organisation maintains a current record of staff and their roles. 4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration. 4.3 All staff understand that their activities on IT systems will be monitored and recorded for security purposes. 4.4 Systems which do not support individual login – either for technical or procedural reasons – are known and a risk and remediation statement is documented for each.	√	√	√		√	√	√				√	√			√					√	√	√	√
14.1-206-CSU Variant	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.	This is covered by NDG Standard 1 Assertions: 4.1 The organisation maintains a current record of staff and their roles. 4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration. 4.3 All staff understand that their activities on IT systems will be monitored and recorded for security purposes. 4.4 Systems which do not support individual login – either for technical or procedural reasons – are known and a risk and remediation statement is documented for each.				√																			
14.1-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	This is covered in NDG Standard 1 Assertion 1.5 Personal information is used and shared lawfully.	√		√	√	√		√				√	√								√	√	√	√
14.1-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	This is covered in NDG Standard 1 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4)	√	√	√	√	√	√	√				√	√			√		√	√	√	√	√	√	√	√
14.1-209-CSU Variant	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	This is covered in NDG Standard 1 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1				√																			
14.1-210	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	This is covered under NDG Standard 1 and 2 Assertion 1.6 The use of personal information is subject to data protection by design and by default. 2.1 There is a clear understanding of what Personal Confidential Information is held.	√	√	√	√	√	√	√				√	√			√					√	√	√	√

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-211	All transfers of personal and sensitive information are conducted in a secure and confidential manner	This is covered under NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully. 1.6 The use of personal information is subject to data protection by design and by default.															√	√								
14.1-212	Consent is appropriately sought before personal information is used in ways that do not directly contribute to the delivery of care services and objections to the disclosure of confidential personal information are appropriately respected	This is covered under NDG Standard 1 Assertions: 1.3 Individuals' rights are respected and supported (GDPR Art 12-22) 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully.														√		√	√	√	√					
14.1-213	There is a publicly available and easy to understand patient information leaflet that informs patients how their information is used, who may have access to that information, and their rights to see and obtain copies of their records	Yes this is included in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. Assertion 1.3 Individuals' rights are respected and supported (GDPR Art 12-22) Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4)																√	√	√	√	√				
14.1-214.1	There is a confidentiality code of conduct that provides staff with clear guidance on the disclosure of personal information	Yes This is covered under NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.														√			√	√	√	√				
14.1-215	All new processes, services and systems are developed and implemented to comply with information security, information quality and confidentiality and data protection requirements	This is covered under NDG Standard 1 Assertion 1.6 The use of personal information is subject to data protection by design and by default																				√				
14.1-216	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	This is covered by NDG Standard 1 Assertions: 4.1 The organisation maintains a current record of staff and their roles. 4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration. 4.3 All staff understand that their activities on IT systems will be monitored and recorded for security purposes. 4.4 Systems which do not support individual login – either for technical or procedural reasons – are known and a risk and remediation statement is documented for each.																				√				

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-220	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	This is covered under NDG Standard 1 Assertions: 1.3 Individuals' rights are respected and supported (GDPR Art 12-22) 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully.													√											
14.1-221	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	This is covered by NDG Standard 4 Assertions: 4.1 The organisation maintains a current record of staff and their roles. 4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration. 4.3 All staff understand that their activities on IT systems will be monitored and recorded for security purposes. 4.4 Systems which do not support individual login – either for technical or procedural reasons – are known and a risk and remediation statement is documented for each.													√											
14.1-222	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	This is covered in NDG Standard 1 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully.													√											
14.1-223	All transfers of personal and sensitive information are conducted in a secure and confidential manner	This is covered under NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully. 1.6 The use of personal information is subject to data protection by design and by default.													√											
14.1-230	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs	Yes this is included in NDG Standard 1 Assertion 1.1 There is senior ownership of data security and protection within the organisation.									√															
14.1-231	Staff are provided with clear guidance on keeping personal information secure, on respecting the confidentiality of service users, and on the duty to share information for care purposes	Yes this is included in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. Assertion 1.5 Personal information is used and shared lawfully. Assertion 2.2 Personal Confidential Information is processed/shared legally and securely. Assertion 2.3 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.									√															

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-232	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	Yes this is included in NDG Standard 1 Assertion 1.3 Individuals' rights are respected and supported (GDPR Art 12-22) 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully.									√															
14.1-234	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	Yes this is covered by NDG Standard 1 Assertion 1.3 Individuals' rights are respected and supported (GDPR Art 12-22)									√															
14.1-235	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.	This is covered by NDG Standard 4 Assertions: 4.1 The organisation maintains a current record of staff and their roles. 4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration. 4.3 All staff understand that their activities on IT systems will be monitored and recorded for security purposes. 4.4 Systems which do not support individual login – either for technical or procedural reasons – are known and a risk and remediation statement is documented for each.									√															
14.1-236	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	This is covered in NDG Standard 1 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully.									√															
14.1-237	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	This is covered under NDG Standard 1 and 2 Assertion 1.6 The use of personal information is subject to data protection by design and by default 2.1 There is a clear understanding of what Personal Confidential Information is held.									√															
14.1-240	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidance	This is covered in NDG Standard 1 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4)										√														
14.1-241	All transfers of personal and sensitive information are conducted in a secure and confidential manner	This is covered under NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully. 1.6 The use of personal information is subject to data protection by design and by default.										√														

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-242	Consent is appropriately sought before personal information is used in ways that do not directly contribute to the delivery of care services and objections to the disclosure of confidential personal information are appropriately respected	This is covered under NDG Standard 1 Assertions: 1.3 Individuals' rights are respected and supported (GDPR Art 12-22) 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully.										√														
14.1-243	There is a publicly available and easy to understand patient information leaflet that informs patients how their information is used, who may have access to that information, and their rights to see and obtain copies of their records	Yes this is included in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 1.3 Individuals' rights are respected and supported (GDPR Art 12-22) 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4).										√														
14.1-244	There is a confidentiality code of conduct that provides staff with clear guidance on the disclosure of personal information	Yes This is covered under NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.										√														
14.1-250	Individuals are informed about the proposed use of their personal information	Yes this is included in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. NDG Standard 1 Assertion 1.3 Individuals' rights are respected and supported (GDPR Art 12-22) NDG Standard 1 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4)								√												√	√	√	√
14.1-251	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs	Yes this is included in NDG Standard 1 Assertion 1.1 There is senior ownership of data security and protection within the organisation.							√																
14.1-252	Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users	Yes this is included in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. Assertion 1.5 Personal information is used and shared lawfully. This also covered in NDG STandard 2 Assertion 2.2 Personal Confidential Information is processed/shared legally and securely. 2.3 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.							√																

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-253	Personal information is shared for care but 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	This is covered under NDG Standard 1 Assertions: 1.3 Individuals' rights are respected and supported (GDPR Art 12-22) 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully.								√																
14.1-254	Individuals are informed about the proposed uses of their personal information	Yes this is included in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 1.3 Individuals' rights are respected and supported (GDPR Art 12-22) 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4)								√																
14.1-255	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	This is covered in NDG Standard 1 Assertion 1.5 Personal information is used and shared lawfully.								√																
14.1-256	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	This is covered under NDG Standard 1 Assertion 1.6 The use of personal information is subject to data protection by design and by default 2.1 There is a clear understanding of what Personal Confidential Information is held.								√																
14.1-300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	Yes this is included in NDG Standard 1 Assertion 1.1 There is senior ownership of data security and protection within the organisation.	√	√	√	√	√	√	√				√	√									√	√	√	√
14.1-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	Yes this is included in NDG Standard 1 and 2 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4). 2.1 There is a clear understanding of what Personal Confidential Information is held.	√	√	√	√	√	√	√				√	√									√	√	√	√
14.1-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	Yes this is included in NDG Standard 6 Assertions 6.1 A confidential system for reporting security breaches and near misses is in place and actively used. 6.2 Users know how to spot an incident and where to report it, and incidents are effectively reported.	√	√	√	√	√	√	√				√	√									√	√	√	√

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority	This is included in the NDG Standard 4 Assertions 4.1 The organisation maintains a current record of staff and their roles. 4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration. **But are not specific to Registration Authority but covered under access control**.	√	√	√	√	√	√				√	√	√									√	√	√	√
14.1-304	Monitoring and enforcement processes are in place to ensure NHS national application smartcard users comply with the terms and conditions of use	This is included in the NDG Standard 4 Assertions 4.3 All staff understand that their activities on IT systems will be monitored and recorded for security purposes. **But are not specific to Registration Authority but covered under access control.**	√	√	√	√	√	√					√	√		√		√	√	√	√	√	√	√	√	√
14.1-305	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	This is included in the NDG Standard 4 Assertions 4.1 The organisation maintains a current record of staff and their roles. 4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration.	√	√	√	√	√	√	√				√	√		√	√						√	√	√	√
14.1-307	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy	This is included in the NDG Standard 4 Assertion 4.3 All staff understand that their activities on IT systems will be monitored and recorded for security purposes. 4.4 Systems which do not support individual login – either for technical or procedural reasons – are known and a risk and remediation statement is documented for each.	√	√	√	√	√	√	√				√	√									√	√	√	√
14.1-308	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	This is covered under NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully. 1.6 The use of personal information is subject to data protection by design and by default.	√	√	√	√	√	√	√				√	√									√	√	√	√
14.1-309	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	This is covered by NDG Standard 6 and 7 Assertions 6.4 Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses. 7.1 There is a continuity plan in place for data security incidents, and staff understand how to put this into action. 7.2 There is an effective annual test of the continuity plan for data security incidents.	√	√	√	√	√	√	√				√	√									√	√	√	√

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	This is covered by NDG Standard 1 and 9 Assertion 1.6 The use of personal information is subject to data protection by design and by default. 9.1 All networking components have had their default passwords changed. 9.2 Web applications owned by the organisation are secured against OWASP Top 10 vulnerabilities. 9.3 All organisations receive a penetration test annually, whether commercially sourced or in-house. The scope of the pen-test is articulated to the SIRO and signed by them. 9.4 A data security improvement plan has been put in place on the basis of the assessment and has been approved by the SIRO.	√	√	√	√	√		√				√	√									√	√	√	√
14.1-311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	This is covered by NDG Standard 1, 2, 6, 8 and 9 Assertion 1.6 The use of personal information is subject to data protection by design and by default. 2.1 There is a clear understanding of what Personal Confidential Information is held. 6.3 All user devices are subject to anti-virus protections while email services benefit from spam filtering deployed at the corporate gateway. 8.1 All software has been surveyed to understand if it is supported and up to date. 8.2 Unsupported software is categorised and documented, and data security risks are identified and managed. 8.3 Supported systems are kept up-to-date with the latest security patches. 9.1 All networking components have had their default passwords changed. 9.2 Web applications owned by the organisation are secured against OWASP Top 10 vulnerabilities. 9.3 All organisations receive a penetration test annually, whether commercially sourced or in-house. The scope of the pen-test is articulated to the SIRO and signed by them. 9.4 A data security improvement plan has been put in place on the basis of the assessment and has been approved by the SIRO.	√	√	√	√	√		√				√	√									√	√	√	√

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	This is covered by NDG Standard 1 and 9 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 9.1 All networking components have had their default passwords changed. 9.3 All organisations receive a security test annually, whether commercially sourced or in-house. The scope of the pen-test is articulated to the SIRO and signed by them. 9.4 A data security improvement plan has been put in place on the basis of the assessment and has been approved by the SIRO.	√	√	√	√	√	√	√				√	√			√						√	√	√	√
14.1-314.1	Policy and procedures ensure that mobile computing and teleworking are secure	Yes this is included in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.	√	√	√	√	√	√	√				√	√		√	√						√	√	√	√
14.1-315	Security management requirements to protect the Airwave communications service are satisfied	Some of the security elements of this requirement are partially covered in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. and 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4). **This is not included as a stand alone anymore as it is not directly aligned with NDG Standards but more .**		√																						
14.1-316	There is an Information Asset Register that includes all key information, software, hardware and services	This is covered by NDG Standard 1 and 2 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4). 2.1 There is a clear understanding of what Personal Confidential Information is held.														√	√	√	√	√	√	√				
14.1-317	Unauthorised access to the premises, equipment, records and other assets is prevented	This is covered by NDG Standard 1 and 2 Assertion 1.6 The use of personal information is subject to data protection by design and by default 2.1 There is a clear understanding of what Personal Confidential Information is held.					√										√	√	√	√	√	√				
14.1-318	The use of mobile computing systems is controlled, monitored and audited to ensure their correct operation and to prevent unauthorised access	This is covered by NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 1.6 The use of personal information is subject to data protection by design and by default																√	√	√	√	√				

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-319	There are documented plans and procedures to support business continuity in the event of power failures, system failures, natural disasters and other disruptions	This is covered by NDG Standard 7 Assertions 7.1 There is a continuity plan in place for data security incidents, and staff understand how to put this into action. 7.2 There is an effective annual test of the continuity plan for data security incidents.														√	√	√	√	√	√	√				
14.1-320	There are documented incident management and reporting procedures	Yes this is included in NDG Standard 6 Assertions; 6.1 A confidential system for reporting security breaches and near misses is in place and actively used. 6.2 Users know how to spot an incident and where to report it, and incidents are effectively reported. 6.4 Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses.														√	√	√	√	√	√	√				
14.1-321	There are appropriate procedures in place to manage access to computer-based information systems	This is included in the NDG Standard 4 Assertions 4.1 The organisation maintains a current record of staff and their roles. 4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration. 4.3 All staff understand that their activities on IT systems will be monitored and recorded for security purposes. 4.4 Systems which do not support individual login – either for technical or procedural reasons – are known and a risk and remediation statement is documented for each.																	√	√	√	√				
14.1-322	All transfers of hardcopy and digital personal and sensitive information have been identified, mapped and risk assessed. Technical and organizational measures adequately secure these transfers	This is covered under NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully. 1.6 The use of personal information is subject to data protection by design and by default.														√			√	√	√	√				
14.1-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	This is covered by NDG Standard 1 and 2 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. and 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.6 The use of personal information is subject to data protection by design and by default 2.1 There is a clear understanding of what Personal Confidential Information is held.	√	√	√	√	√	√	√			√	√			√	√						√	√	√	√

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	This is covered by NDG Standard 1 Assertion 1.6 The use of personal information is subject to data protection by design and by default	√		√	√	√	√	√				√	√									√	√	√	√
14.1-325	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	This is covered by NDG Standard 1 and 9 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 9.1 All networking components have had their default passwords changed. 9.3 All organisations receive a security test annually, whether commercially sourced or in-house. The scope of the pen-test is articulated to the SIRO and signed by them. 9.4 A data security improvement plan has been put in place on the basis of the assessment and has been approved by the SIRO.																				√				
14.1-330	Policy and procedures ensure that mobile computing and teleworking are secure	This is covered by NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.													√											
14.1-331	There is an information asset register that includes all key information, software, hardware and services	This is covered by NDG Standard 1 and 2 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 2.1 There is a clear understanding of what Personal Confidential Information is held.													√											
14.1-332	Unauthorised access to the premises, equipment, records and other assets is prevented	This is covered by NDG Standard 1 and 2 Assertion 1.6 The use of personal information is subject to data protection by design and by default 2.1 There is a clear understanding of what Personal Confidential Information is held.													√											
14.1-333	There are documented incident management and reporting procedures	Yes this is included in NDG Standard 6 Assertions; 6.1 A confidential system for reporting security breaches and near misses is in place and actively used. 6.2 Users know how to spot an incident and where to report it, and incidents are effectively reported.													√											
14.1-334	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	This is covered by NDG Standard 1 Assertion 1.6 The use of personal information is subject to data protection by design and by default													√											
14.1-335	There are adequate safeguards in place to ensure that all patient/client information is processed securely within a safe haven environment distinct from other areas of organisational activity.	This is covered by NDG Standard 1 Assertion 1.6 The use of personal information is subject to data protection by design and by default													√								√	√	√	√

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-340	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	Yes this is included in NDG Standard 1 and 3 Assertion 1.1 There is senior ownership of data security and protection within the organisation. 3.1 There has been an assessment of data security and protection training needs across the organisation.									√															
14.1-341	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	Yes this is included in NDG Standard 1 and 2 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 2.1 There is a clear understanding of what Personal Confidential Information is held.									√															
14.1-342	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority	This is included in the NDG Standard 4 Assertions 4.1 The organisation maintains a current record of staff and their roles. 4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration. **But are not specific to Registration Authority but covered more generally under access control.**									√															
14.1-343	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use	This is included in the NDG Standard 4 Assertions 4.3 All staff understand that their activities on IT systems will be monitored and recorded for security purposes. **But are not specific to Registration Authority but covered more generally under access control.**									√															
14.1-344	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	This is included in the NDG Standard 4 Assertions 4.1 The organisation maintains a current record of staff and their roles. 4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration.									√															
14.1-345	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy	This is covered under NDG Standard 1 Assertion 1.1 There is senior ownership of data security and protection within the organisation.									√															
14.1-346	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	This is covered by NDG Standard 6 and 7 Assertions 6.4 Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses. 7.1 There is a continuity plan in place for data security incidents, and staff understand how to put this into action. 7.2 There is an effective annual test of the continuity plan for data security incidents.									√															

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-347	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	This is covered by NDG Standard 1 and 9 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 9.1 All networking components have had their default passwords changed. 9.3 All organisations receive a security test annually, whether commercially sourced or in-house. The scope of the pen-test is articulated to the SIRO and signed by them. 9.4 A data security improvement plan has been put in place on the basis of the assessment and has been approved by the SIRO.									√																
14.1-348	Policy and procedures ensure that mobile computing and teleworking are secure	This is covered by NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.									√															
14.1-349	There are documented incident management and reporting procedures	Yes this is included in NDG Standard 6 Assertions; 6.1 A confidential system for reporting security breaches and near misses is in place and actively used. 6.2 Users know how to spot an incident and where to report it, and incidents are effectively reported.									√															
14.1-350	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	This is covered under NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully. 1.6 The use of personal information is subject to data protection by design and by default.									√															
14.1-351	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	This is covered by NDG Standard 1 and 2 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. and 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.6 The use of personal information is subject to data protection by design and by default 2.1 There is a clear understanding of what Personal Confidential Information is held.									√															
14.1-352	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	This is covered by NDG Standard 1 Assertion 1.6 The use of personal information is subject to data protection by design and by default									√															

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-360	Monitoring and enforcement processes are in place to ensure NHS national application smartcard users comply with the terms and conditions of use	This is included in the NDG Standard 4 Assertions 4.3 All staff understand that their activities on IT systems will be monitored and recorded for security purposes. **But are not specific to Registration Authority but covered more generally under access control.**										√														
14.1-361	There is an Information Asset Register that includes all key information, software, hardware and services	This is covered by NDG Standard 1 and 2 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 2.1 There is a clear understanding of what Personal Confidential Information is held.										√														
14.1-362	Unauthorised access to the premises, equipment, records and other assets is prevented	This is covered by NDG Standard 1 and 2 Assertion 1.6 The use of personal information is subject to data protection by design and by default 2.1 There is a clear understanding of what Personal Confidential Information is held.										√														
14.1-363	The use of mobile computing systems is controlled, monitored and audited to ensure their correct operation and to prevent unauthorised access	This is covered by NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 1.6 The use of personal information is subject to data protection by design and by default.										√														
14.1-364	There are documented plans and procedures to support business continuity in the event of power failures, system failures, natural disasters and other disruptions	This is covered by NDG Standard 7 Assertions 7.1 There is a continuity plan in place for data security incidents, and staff understand how to put this into action. 7.2 There is an effective annual test of the continuity plan for data security incidents.										√														
14.1-365	There are documented incident management and reporting procedures	Yes this is included in NDG Standard 6 Assertions; 6.1 A confidential system for reporting security breaches and near misses is in place and actively used. 6.2 Users know how to spot an incident and where to report it, and incidents are effectively reported.										√														
14.1-366	There are appropriate procedures in place to manage access to computer-based information systems	This is included in the NDG Standard 4 Assertions 4.1 The organisation maintains a current record of staff and their roles. 4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration. 4.3 All staff understand that their activities on IT systems will be monitored and recorded for security purposes. 4.4 Systems which do not support individual login – either for technical or procedural reasons – are known and a risk and remediation statement is documented for each.										√														

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-367	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	This is covered by NDG Standard 1 and 9 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 9.1 All networking components have had their default										√														
14.1-370	Key Information Governance requirements for processing confidential personal data are being met	This is covered by NDG Standard 1 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.6 The use of personal information is subject to data protection by design and by default																							√	
14.1-371	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	Yes this is included in NDG Standard 1 and 3 Assertion 1.1 There is senior ownership of data security and protection within the organisation. 3.1 There has been an assessment of data security and protection training needs across the organisation.								√																
14.1-372	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	Yes this is included in NDG Standard 1 and 2 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4). 2.1 There is a clear understanding of what Personal Confidential Information is held.								√																
14.1-373	There are documented information security incident / event reporting and management procedures that are accessible to all staff	Yes this is included in NDG Standard 6 Assertions 6.1 A confidential system for reporting security breaches and near misses is in place and actively used. 6.2 Users know how to spot an incident and where to report it, and incidents are effectively reported.								√																
14.1-374	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	This is included in the NDG Standard 4 Assertions 4.1 The organisation maintains a current record of staff and their roles. 4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration.								√																
14.1-375	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	This is covered under NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.5 Personal information is used and shared lawfully. 1.6 The use of personal information is subject to data protection by design and by default.								√																

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-376	Business continuity plans are up to date and tested for all critical information assets (e.g. data processing facilities, communications services and data) and service - specific measures are in place	This is covered by NDG Standard 6 and 7 Assertions 6.4 Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses. 7.1 There is a continuity plan in place for data security incidents, and staff understand how to put this into action. 7.2 There is an effective annual test of the continuity plan for data security incidents.								√																
14.1-377	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error.	This is covered by NDG Standard 1 and 9 Assertion 1.6 The use of personal information is subject to data protection by design and by default. 9.1 All networking components have had their default passwords changed. 9.2 Web applications owned by the organisation are secured against OWASP Top 10 vulnerabilities. 9.3 All organisations receive a penetration test annually, whether commercially sourced or in-house. The scope of the pen-test is articulated to the SIRO and signed by them. 9.4 A data security improvement plan has been put in place on the basis of the assessment and has been approved by the SIRO.								√																
14.1-378	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	This is covered by NDG Standard 1, 2, 6, 8 and 9 Assertion 1.6 The use of personal information is subject to data protection by design and by default. 2.1 There is a clear understanding of what Personal Confidential Information is held. 6.3 All user devices are subject to anti-virus protections while email services benefit from spam filtering deployed at the corporate gateway. 8.1 All software has been surveyed to understand if it is supported and up to date. 8.2 Unsupported software is categorised and documented, and data security risks are identified and managed. 8.3 Supported systems are kept up-to-date with the latest security patches. 9.1 All networking components have had their default passwords changed. 9.2 Web applications owned by the organisation are secured against OWASP Top 10 vulnerabilities. 9.3 All organisations receive a penetration test annually, whether commercially sourced or in-house. The scope of the pen-test is articulated to the SIRO and signed by them. 9.4 A data security improvement plan has been put in place on the basis of the assessment and has been approved by the SIRO.								√																

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-379	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	This is covered by NDG Standard 1 and 9 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 9.1 All networking components have had their default								√																
14.1-380	Policy and procedures ensure that mobile computing and teleworking are secure	This is covered by NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.								√																
14.1-381	There is an information asset register that includes all key information, software, hardware and services	This is covered by NDG Standard 1 and 2 Assertion 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 2.1 There is a clear understanding of what Personal Confidential Information is held.								√																
14.1-382	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	This is covered by NDG Standard 1 and 2. Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. and 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4) 1.6 The use of personal information is subject to data protection by design and by default 2.1 There is a clear understanding of what Personal Confidential Information is held.								√																
14.1-383	The confidentiality of service user information that is not involved in the process of providing direct care is protected through use of pseudonymisation and anonymisation techniques where appropriate	This is covered by NDG Standard 1 Assertion 1.6 The use of personal information is subject to data protection by design and by default								√																
14.1-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	Yes this is included in NDG Standard 1 and 3 Assertion 1.1 There is senior ownership of data security and protection within the organisation. 3.1 There has been an assessment of data security and protection training needs across the organisation.	√	√	√	√	√	√	√				√	√									√	√	√	√
14.1-401	There is consistent and comprehensive use of the NHS number in line with the National Patient Safety Agency requirements	**NHS Number Not covered separately in the DSPT Standard but forms a minor part of the data quality** Assertion 1.7 Effective data quality controls are in place **NHS Number Standard is a separate standard in its own right ISB 0149.**	√	√	√			√					√	√									√	√	√	√
14.1-401-CSU Variant	There is consistent and comprehensive use of the NHS number in line with the National Patient Safety Agency requirements	**NHS Number Not covered separately in the DSPT Standard but forms a minor part of the data quality** Assertion 1.7 Effective data quality controls are in place **NHS Number Standard is a separate standard in its own right ISB 0149.**				√																				
14.1-402	Procedures are in place to ensure the accuracy of service user information on all systems that support the provision of care	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place	√	√	√			√					√	√		√									√	
14.1-402-CSU Variant	Procedures are in place to ensure the accuracy of service user information on all systems that support the provision of care	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place				√																				

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-404	A multi-professional audit of clinical records across all specialties has been undertaken	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place	√	√	√									√		√										
14.1-404-CSU Variant	A multi-professional audit of clinical records across all specialties has been undertaken	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place				√																				
14.1-406	Procedures are in place for monitoring the availability of paper care records and tracing missing records	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place	√		√									√												
14.1-406-CSU Variant	Procedures are in place for monitoring the availability of paper care records and tracing missing records	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place				√																				
14.1-412	Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care, support and advisory services	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place																				√				
14.1-420	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	Yes this is included in NDG Standard 1 and 3 Assertion 1.1 There is senior ownership of data security and protection within the organisation. 3.1 There has been an assessment of data security and protection training needs across the organisation.									√															
14.1-421	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	**NHS Number Not covered separately in the DSPT Standard but forms a minor part of the data quality** Assertion 1.7 Effective data quality controls are in place **NHS Number Standard is a separate standard in its own right ISB 0149.**									√															
14.1-430	Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care, support and advisory service	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place										√														
14.1-440	An information quality assurance programme is in place to drive improvements across the organisation	This is covered in part NDG Standard 1 Assertion 1.1 There is senior ownership of data security and protection within the organisation. 1.7 Effective data quality controls are in place																					√	√	√	√
14.1-441	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	Yes this is included in NDG Standard 1 and 3 Assertion 1.1 There is senior ownership of data security and protection within the organisation. 3.1 There has been an assessment of data security and protection training needs across the organisation.								√																
14.1-442	There is consistent and comprehensive use of the NHS Number in line with National Policy requirements	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place								√																
14.1-443	Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place								√																
14.1-444	Procedures are in place for monitoring the availability of paper service user records and tracing missing records	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place								√																
14.1-501	National data definitions, standards, values and validation programmes are incorporated within key systems and local documentation is updated as standards develop	**This is partially covered in NDG Standard 1** Assertion 1.7 Effective data quality controls are in place **But does not cover all the existing requirement**	√		√	√							√	√										√		

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-502	External data quality reports are used for monitoring and improving data quality	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place **But it does not mandate the specific requirement to use external DQ reports**	√		√	√							√	√											√	
14.1-504	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	**This is minimally covered in NDG Standard 1** Assertion 1.7 Effective data quality controls are in place **But it does not mandate the specific requirement to use benchmarking.**	√		√	√																			√	
14.1-505	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	**This is partially covered in NDG Standard 1** Assertion 1.7 Effective data quality controls are in place **But it does not mandate the clinical coding audit.**	√																							
14.1-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place **But it does not mandate the clinical coding audit.**	√		√																					
14.1-507	The Completeness and Validity check for data has been completed and passed	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place **But it does not mandate the Completeness and Validity check.**	√		√																					
14.1-508	Clinical/care staff are involved in validating information derived from the recording of clinical/care activity	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place **But it does not mandate that Clinicians are involved in validating data.**	√		√																					
14.1-510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national clinical coding standards	This is covered in NDG Standard 3 Assertion 3.4 Staff with specialist roles receive data security and protection training suitable to their role.	√																							
14.1-514.1	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	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place **But it does not specifically mandate the clinical coding audit.**			√																					
14.1-515	There is a robust programme of internal and external data quality audit	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place				√																				
14.1-516	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national clinical coding standards	This is covered in NDG Standard 3 Assertion 3.4 Staff with specialist roles receive data security and protection training suitable to their role.			√																					
14.1-601	Documented and implemented procedures are in place for the effective management of corporate records	This is covered in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 1.8 Personal information processed by the organisation is adequate (and not excessive) for the purposes. **This covers all records and not just corporate ones.**	√	√	√	√	√		√				√										√	√	√	√

Version 14.1 IGT sequence number	Requirement Statement	In scope of DSPT Toolkit	ACUTE	AMT	MHT	CSU	NHSBSA	NHSBP	SUO	LA	CCG	AQP:	AQP: CLIN	CHP	HSUT/P	PH	CTP	GP	PHARM/DA	DEN	EYECARE	VOL	NHSE	NHSD	PHE	DSC
14.1-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	This is covered in NDG Standard 1 Assertion 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. 1.3 Individuals' rights are respected and supported (GDPR Art 12-22) .	√	√	√	√	√		√					√										√	√	√	√
14.1-604	As part of the information lifecycle management strategy, an audit of all corporate records has been undertaken	This is covered in NDG Standard 1 Assertion 1.7 Effective data quality controls are in place. **This covers all records and not just corporate ones.**	√	√	√	√	√		√					√										√	√	√	√
New	N/A	**New Requirement** 5.1 Process reviews are held at least once per year.																								
New		**New Requirement** 5.2 Participation in reviews is comprehensive, and clinicians are actively involved.																								
New		**New Requirement** 5.3 Action is taken to address problem processes as a result of feedback at meetings or in year.																								
Partial		**New Requirement** 8.1 All software has been surveyed to understand if it is supported and up to date.																								
Partial		**New Requirement** 8.2 Unsupported software is categorised and documented, and data security risks are identified and managed.																								
New		**New Requirement** 9.2 Web applications owned by the organisation are secured against OWASP Top 10 vulnerabilities..																								