

INFORMATION MANAGEMENT ASSURANCE CHECKLIST

In conjunction with the organisation's Senior Information Risk Owner and Personal Data Guardian, as Chief Executive of [*insert name of organisation*], I hereby give an assurance that a systematic and planned approach to the governance of information is in place that ensures the organisation can maintain information in a manner that effectively services its needs and those of its stakeholders in line with appropriate legislation.

I can confirm that:

	YES/NO
1. IG FRAMEWORK	
i) My organisation has in place an Information Governance Management Framework which is supported by policies, strategies and improvement plans.	
ii) My organisation has in place Information Governance awareness and mandatory training procedures and staff are appropriately trained.	
iii) The Information Governance agenda in my organisation is supported by adequate information quality and records management skills, knowledge and experience.	
iv) My organisation's SIRO is effectively supported and takes ownership of the organisation's information risk policy and management strategy.	
v) My organisation has documented and agreed procedures in place to ensure compliance with the requirements of the General Data Protection Regulation (GDPR).	
2. FOI/EIR	
i) My organisation has documented and publicly available procedures in place to ensure compliance with the Freedom of Information (FOI) Act 2000 and Environmental Information Regulations 2004 (EIR).	
3. DATA PROTECTION AND CONFIDENTIALITY	
i) All staff in my organisation are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users.	
ii) Information Governance in my organisation is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs.	

iii)	In my organisation there are appropriate procedures in place for recognising and responding to individuals' requests for access to their personal data.
iv)	Individuals are informed about the proposed uses of their personal information which is held by my organisation.
v)	Processing outside the UK of person identifiable data held by my organisation complies with the General Data Protection Regulation and Department of Health (NI) guidelines.
vi)	The processes for all transfers of hardcopy and digital person identifiable and sensitive information held by my organisation have been identified, mapped and risk assessed, and technical and organisational measures adequately secure these transfers.
vii)	The confidentiality of service user information held by my organisation is protected through use of pseudonymisation and anonymisation techniques where appropriate.
4. THIRD PARTIES	
i)	My organisation has contractual arrangements in place with all contractors, support organisations and individuals carrying out work on behalf of the organisation which include compliance with information governance & relevant legislative requirements.
ii)	In situations where the use of personal information held by my organisation does not directly contribute to the delivery of care services such information is only processed where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected.
iii)	Where required, protocols governing the sharing of personal information by my organisation have been agreed with the other organisation.
5. MANAGEMENT OF CLINICAL RECORDS	
i)	In my organisation there is consistent and comprehensive use of the Health + Care Number (HCN) in line with the Department's best practice guidance.
ii)	Procedures are in place in my organisation to ensure the accuracy of service user information on all systems and/or records that support the provision of care.
iii)	A multi-professional audit of clinical and social care records across all specialties has been undertaken in my organisation.

iv)	Procedures are in place within my organisation for monitoring the availability of paper health/care records and tracing missing records.	
v)	In my organisation national data definitions, standards and validation programmes are incorporated within key systems and local documentation is updated as standards develop.	
vi)	External data quality reports are used for monitoring and improving data quality within my organisation.	
vii)	In my organisation audits of clinical coding, based on national standards, have been undertaken by a NHS Classifications Service approved clinical coding auditor within the last 12 months.	
viii)	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place within my organisation.	
ix)	In my organisation clinical/care staff are involved in validating information derived from the recording of clinical/care activity.	
x)	In my organisation training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national standards.	
6. MANAGEMENT OF CORPORATE RECORDS		
i)	Documented and implemented procedures are in place for the effective management of corporate records in my organisation.	
ii)	As part of the information lifecycle management strategy, an audit of corporate records held by my organisation has been undertaken and an Information Asset Register is maintained.	

If you are unable to provide any of these assurances, please explain what the current circumstances are on a separate page and detail what action is being taken to resolve the issues including timeframes.

This information should be returned to the Department.

Signed:
Chief Executive
Organisation:
Date: