INFORMATION MANAGEMENT

STANDARD

A systematic and planned approach to the Governance of Information is in place within the organisation 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.

OVERVIEW

Information, as we know it today, includes both electronic and physical information. The organisational structure must be capable of managing this information throughout the information lifecycle regardless of source or format. Information management is a corporate responsibility that needs to be addressed and followed from the uppermost senior levels of management to the front line worker. Organisations must be held and must hold its employees accountable to capture, manage, store, share, preserve and deliver information appropriately and responsibly. Part of that responsibility lies in training the organisation to become familiar with the policies, processes, technologies and best practices in Information Management.

This Information Management standard requires organisations to carry out self assessments of their compliance against the criterion, to determine whether their information is managed correctly.

The Data Protection Act 1998 supported by other access to information regimes such as the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Access to Health Records (Northern Ireland) Order 1993 impacts significantly on the record keeping arrangements in public authorities.

Health and Social Care (HSC) bodies must ensure that information and records management policies and procedures are fully compliant with legislation and government policy on the management of information. Further information can be accessed at http://www.proni.gov.uk.

It is also important to manage the different risks associated with the various systems of data capture, recording, retrieval and disposal and for these to be controlled, i.e. paper based systems may require different controls than those which are computer based, although the underlying principles of confidentiality etc will remain common. It is also essential for any assessment to consider the potential variation in records management across the organisation (in that different organisations may well have historically different records management systems, especially if there is no previous history of working together). Ensuring that all organisations comply with relevant policies and legislation and maintain the highest standards of data management is central to the achievement of the organisation's objectives.

Creating and maintaining electronic records for both service user[1] services and administration can offer significant benefits, but also substantial challenges. Records management strategies need to take account of the developing Health Records Infrastructure, including measures for ensuring the confidentiality, integrity, availability and disposal of records.

Information is the lifeblood of organisations and is essential to the delivery of high quality evidence-based health care on a day-to-day basis. Records are a valuable resource because of the information they contain. That information is only usable if it is correctly recorded in the first place, is regularly updated, properly stored and maintained, and is easily accessible when needed.

Given the value of information it is important that it is appropriately incorporated within the organisation's business continuity plans.

It should be noted that any lists of examples throughout this standard are not exhaustive.

Compliance

The table below sets out the compliance levels expected against each criterion in 2016 – 2017.

Criterion	Compliance required 2013-2014	Compliance Required 2014-2015	Compliance Required 2015-2016	Compliance Required 2016-2017
1	Moderate	Moderate	Substantive	Substantive
2	Substantive Whilst this has not been measured before through Controls Assurance, SIROs should be in place and performing to the level required in this criteria.	Substantive	Substantive	Substantive
3	Substantive	Substantive	Substantive	Substantive
4	Substantive	Substantive	Substantive	Substantive
5	Substantive	Substantive	Substantive	Substantive
6	Substantive	Substantive	Substantive	Substantive
7	Substantive	Substantive	Substantive	Substantive
8	Moderate	Substantive	Substantive	Substantive
9	Moderate	Moderate	Moderate	Substantive
10	Substantive	Substantive	Substantive	Substantive
11	Substantive	Substantive	Substantive	Substantive
12	Substantive	Substantive	Substantive	Substantive

[1] Service User – Service User in clinical terms refers to anyone who uses health or social care services but it equally applies to staff. A service user is anyone who uses a service whether that be clinical or corporate.

13	Substantive	Substantive	Substantive	Substantive
14	Substantive	Substantive	Substantive	Substantive
15	Moderate	Substantive	Substantive	Substantive
16	Moderate	Moderate	Moderate	Substantive
17	Measurement against this criterion is required in 2013 – 2014. It will not however be formally included in the overall compliance with the standard for this year.	Moderate	Substantive	Substantive
18	Moderate	Substantive	Substantive	Substantive
19	Moderate	Moderate	Moderate	Substantive
20	Moderate	Moderate	Moderate	Substantive
21	Substantive	Substantive	Substantive	Substantive
22	This criteria will not be measured against community information in 2013/2014 but Moderate compliance will be required against acute information	Moderate	Substantive	Substantive
23	Moderate	Moderate	Substantive	Substantive
24	Substantive	Substantive	Substantive	Substantive
25	Moderate	Moderate	Moderate	Substantive
26	Moderate	Substantive	Substantive	Substantive
27	Moderate	Substantive	Substantive	Substantive

KEY REFERENCES

- Audit Commission Setting the Record Straight: A Review of Progress in Health Records Services November 1999 **ISBN: 1862401888**

- Audit Commission: Data Remember - Improving The Quality of Patient-Based Information 2002

- Cabinet Office HMG Security Policy Framework Version 10 – April 2013 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200552/HMG_Security_Policy_Framework_v10_0_Apr-2013.pdf

- Reporting and follow-up on serious adverse incidents: http://www.hscboard.hscni.net/publications/Policies/102%20Procedure_for_the_reporting_and_followup_of_Serious_Adverse_Incidents-Oct2013.pdf

- Common Law duty of Confidentiality[2] (see http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/publicationsandstatistics/publications/publicationspolicyandguidance/browsable/DH_5803173)

- Crest The protocol for the hospital transfer of patients and their records August 2006 ISBN 1-903982-23-5 http://www.gain-ni.org/images/Uploads/Guidelines/protocol.pdf

- Department for Health Good Practice Guidelines for GP electronic patient records v4 (2011) https://www.gov.uk/government/publications/the-good-practice-guidelines-for-gp-electronic-patient-records-version-4-2011

- Department of Health Information Governance
- http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igap/dnletter1

- Department of Health, The Information Governance Review, To Share or not to Share © Crown copyright 2013, 2900774 March 2013 Produced by Williams Lea.

- Department for Health Letter from David Nicholson to Chief Executives of NHS Trusts Information Governance and Transfers of Data December 2007
- http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igap/dnletter1

- DHSSPS AMCC 2649 Letter dated 22/09/10 to Chief Executives of HSC Organisations – Senior Information Risk Owner and Information Asset Owner from A McCormick

[2] Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence, it is also referred to as 'judge-made' or case law. The law is applied by reference to those previous cases, so common law is also said to be based on precedent.

- DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information January 2012 https://www.health-ni.gov.uk/publications/code-practice-protecting-confidentiality-service-user-information
- DHSSPS Guidelines for Managing Records in Health and Personal Social Services Organisations in Northern Ireland – Good Management Good Records November 2011 https://www.health-ni.gov.uk/topics/good-management-good-records
- DHSSPS HPSS ICT Programme, From Vision to Reality, March 2005

- DHSSPS & HSC Protocol for Sharing Service User Information for Secondary Purposes August 2011 https://www.dhsspsni.gov.uk/publications/dhssps-hsc-protocol-sharing-service-user-information-secondary-purposeS
- DHSSPS Reference Guide to Consent for Examination, Treatment or Care March 2003 http://www.dhsspsni.gov.uk/consent-referenceguide.pdf

- DHSSPS The Quality Standards for Health and Social Care Supporting Good Governance and Best Practice in the HSC, March 2006

DHSSPS S&Q Learning Communication 05/09: Risk to patient safety of not using the H+C Number as the regional identifier for all patients and clients

https://www.dhsspsni.gov.uk/sites/default/files/publications/dhssps/HSC%20SQSD%20Learning%20Communication%2005-09_0.pdf

-
- General Medical Council, Guidance for Doctors Confidentiality October 2009 http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp
- Great Britain Department of Health 1997 The Caldicott Report, Review of Patient Identifiable Information Recommendation 2 http://www.google.co.uk/url?url=http://webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/%40dh/%40en/documents/digitalasset/dh_4068404.pdf&rct=j&frm=1&q=&esrc=s&sa=U&ei=xJHkVOCsFpPqaJPwgYgF&ved=0CBQQFjAA&usg=AFQjCNGlrEb5TnxzJPg_5AIzG78tp8Cl-w

- Great Britain Department of Health, Health service circular 1999/012 Caldicott Guardians http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Publicationsandstatistics/Lettersandcirculars/Healthservicecirculars/DH_4004311

- Great Britain Department of Health Health service circular 2000/009 Data Protection Act 1998: protection and use of patient information http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Publicationsandstatistics/Lettersandcirculars/Healthservicecirculars/DH_4002964

- Great Britain Department of Health The Caldicott Guardian Manual 2010 http://systems.hscic.gov.uk/infogov/links/2010cgmanual.pdf

- Great Britain. Lord Chancellors Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000. (2009) London: The Lord Chancellor's Department. http://www.nationalarchives.gov.uk/information-management/projects-and-work/records-management-code.htm

- Great Britain (2000) Regulation of Investigatory Powers Act 2000 The Stationery Office London http://www.legislation.gov.uk/ukpga/2000/23/contents

- Great Britain (2000) Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 The Stationery Office London http://www.legislation.gov.uk/uksi/2000/2699/contents/made

- Great Britain (1998) the Data Protection Act 1998 The Stationery Office, London http://www.legislation.gov.uk/ukpga/1998/29/contents

- Great Britain (2000) The Data Protection (Subject Access Modification) (Social Work) Order 2000 The Stationery Office London http://www.legislation.gov.uk/uksi/2000/415/contents/made

- Great Britain (1925) Disposal of Documents Order, 1925 http://www.proni.gov.uk/1925_disposal_of_documents_order.pdf

- Great Britain The Data Protection (Subject Access Modification) (Social Work) Order 2000 The Stationery Office London http://www.legislation.gov.uk/uksi/2000/415/contents/made

- Great Britain (2004) Environmental Information Regulations 2004 The Stationery Office, London http://www.legislation.gov.uk/uksi/2004/3391/contents/made

- Great Britain (2000) The Freedom of Information (FOI) Act 2000 The Stationery Office, London http://www.legislation.gov.uk/ukpga/2000/36/contents

- Great Britain (2004)The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 The Stationery Office, London http://www.legislation.gov.uk/uksi/2004/3244/contents/made

- Great Britain (1998) the Human Rights Act 1998 The Stationary Office London http://www.legislation.gov.uk/ukpga/1998/42/contents

- Great Britain (2003) the Privacy and Electronic Communications (EC Directive) Regulations 2003 The Stationery Office, London http://www.legislation.gov.uk/uksi/2003/2426/contents/made

- Great Britain (2011) The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations The Stationery Office, London 2011 http://www.legislation.gov.uk/uksi/2011/1208/contents/made

- Great Britain (1923) The Public Records Act (NI) 1923 The Stationery Office, London http://www.legislation.gov.uk/apni/1923/20

- HM Government – Cabinet Office Data Handling Procedures in Government: Final Report June 2008 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60966/final-report.pdf

- Information Commissioner Data Protection Audit Manual https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ICO_Data%20Protection%20Audit%20Manual.pdf

- Information Commissioner's Office Anonymisation: Managing Data Protection Risk Code of Practice November 2012 http://www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation

- Information Commissioner's Office Data Protection Act 1998 – Legal Guidance (version 1 as print date) http://www.valident.co.uk/wp-content/uploads/2012/01/data_protection_act_legal_guidance.pdf

- Information Commissioner's Office **The eighth data protection principle and international data transfers**
  The Information Commissioner's recommended approach to assessing adequacy including consideration of the issue of contractual solutions, binding corporate rules and Safe Harbor.
  https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf

- Information Commissioner's Office Data Sharing Code of Practice May 2011 http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx

- Information Commissioner's Office Guidance for Health Sector Organisations http://www.ico.org.uk/for_organisations/sector_guides/health

- Information Commissioner's Office Information Commissioner's guidance about the Issue of Monetary Penalties prepared and issued under section 55C(1) of the Data Protection Act 1998 The Stationary Office London ISBN 9780108511240 http://www.official-documents.gov.uk/document/other/9780108511240/9780108511240.asp

- Institute of Health Records and Information Management provides guidance for its members http://www.ihrim.co.uk/

- International Standard Organisation International Standard ISO 15489 1:2001(E) Information and Documentation – Records Management http://www.iso.org/iso/catalogue_detail?csnumber=31908

- International Standards Organisation BSO ISO/IEC 27000 Series of Information Security Standards http://www.27000.org/

- ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management http://www.iso27001security.com/html/27002.html

- National Health Service The Essence of Care Benchmarks for Record Keeping 2010 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/153468/dh_119965.pdf.pdf

- National Patient Safety Agency Safer Practice Notice 24: Standardising wristbands improves patient safety http://www.nrls.npsa.nhs.uk/resources/?EntryId45=59824

- Northern Ireland Audit Office report – Compensation payments for Clinical negligence 5 July 2002 http://www.niauditoffice.gov.uk/a-to-z.htm/report_archive_2002_clinicalnegligence

- Northern Ireland: HPSS: The NI Data Dictionary http://hscb.sharepoint.hscni.net/sites/pmsi/isdq/SitePages/DataDictionary.aspx

- Northern Ireland Social Care Council Standards of Conduct and Practice http://niscc.info/news/27-whats-new-in-the-niscc-standards-focus-on-the-consultation-process

- Nursing and Midwifery Council The Code, Standards of Conduct performance and ethics for nurses and midwives May 2008 http://www.nmc-uk.org/Nurses-and-midwives/Standards-and-guidance1/The-code/The-code-in-full/

- Public Record Office Northern Ireland (PRONI) – Northern Ireland Records Management Standard https://www.nidirect.gov.uk/articles/records-management-public-bodies

- Royal College Physicians: Generic Medical Record Keeping Standards, https://www.rcplondon.ac.uk/resources/generic-medical-record-keeping-standards
- UK Council for Health Informatics Professionals Code of Conduct http://www.ukchip.org/?q=page/UKCHIP-Code-Conduct

Criterion 1	There is an Information Governance Management Framework supported by policies, strategies and improvement plans which sets out how the organisation manages Information Governance
Criterion 2	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy
Criterion 3	Documented and implemented procedures are in place for the effective management of corporate records
Criterion 4	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information (FOI) Act 2000 and Environmental Information Regulations 2004 (EIR)
Criterion 5	Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users
Criterion 6	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained
Criterion 7	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs
Criterion 8	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience
Criterion 9	Contractual arrangements that include compliance with information governance requirements are in place with all contractors, support organisations and individuals carrying out work on behalf of the organisation
Criterion 10	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken
Criterion 11	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data
Criterion 12	In situations where the use of personal information does not directly contribute to the delivery of care services, such information must only be processed where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected.
Criterion 13	Individuals are informed about the proposed uses of their personal information
Criterion 14	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations

Criterion 15 All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines

Criterion 16 The processes for 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

Criterion 17 The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate

Criterion 18 There is consistent and comprehensive use of the Health+Care Number (HCN) in line with the Department's best practice guidance

Criterion 19 Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care

Criterion 20 A multi-professional audit of clinical records across all specialties has been undertaken

Criterion 21 Procedures are in place for monitoring the availability of paper health/care records and tracing missing records

Criterion 22 National data definitions, standards and validation programmes are incorporated within key systems and local documentation is updated as standards develop

Criterion 23 External data quality reports are used for monitoring and improving data quality

Criterion 24 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

Criterion 25 A documented procedure and a regular audit cycle for accuracy checks on service user data is in place

Criterion 26 Clinical /care staff are involved in validating information derived from the recording of clinical /care activity

Criterion 27 Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national standards

Criterion 1

There is an Information Governance Management Framework supported by policies, strategies and improvement plans which sets out how the organisation manages Information Governance

INFORMATION

Criterion Description

Responsibility for IG rests with the most senior level of accountability, for example, in an HSC organisation this will be the Board. A robust framework for managing IG should extend throughout the organisation. Organisations need clear policies and strategies covering all aspects of the IG agenda approved by the senior management tier so that staff understand both the spirit and the detail of what they are expected to do.

Source

- **DHSSPS Guidelines for Managing Records in** Health and Personal Social Services Organisations in Northern Ireland – Good Management Good Records November 2011.
  https://www.health-ni.gov.uk/topics/good-management-good-records

- DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information January 2012.
- https://www.health-ni.gov.uk/publications/code-practice-protecting-confidentiality-service-user-informationCabinet Office – (May 2010) HMG Information Assurance Maturity Model and Assessment Framework https://www.cesg.gov.uk/articles/hmg-ia-maturity-model-iamm
- Great Britain. Lord Chancellors Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000. (2009) London: The Lord Chancellor's Department.
  http://www.nationalarchives.gov.uk/information-management/projects-and-work/records-management-code.htm

- ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management
  http://www.iso27001security.com/html/27002.html

- Procedure for the Reporting and Follow up of Serious Adverse Incidents
  http://www.hscboard.hscni.net/publications/Policies/102%20Procedure_for_the_reporting_and_followup_of_Serious_Adverse_Incidents-Oct2013.pdf

GUIDANCE

The Information Governance Management Framework

1. Robust IG requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. The way that an organisation chooses to deliver against these requirements is referred to as the organisation's Information Governance Management Framework. This Framework must be documented, approved at the most appropriate senior management level in the organisation (e.g. the Board (or equivalent), senior management team) and reviewed annually.

2. The Information Governance Management Framework may be described in a single one page standalone document or incorporated within an over-arching IG Policy or an IG Strategy and should provide a summary/overview of how an organisation is addressing the IG agenda (see example below).

INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK		
Heading	**Requirement**	**Notes**
Senior Roles	• IG Lead (see below) • Senior Information Risk Owner (SIRO) **(see criteria 2)** • Personal Data Guardian **(see criteria 7)**	These roles should be at Board or the most senior leadership team level
Key Policies **(see criteria 1)**	• Over-arching IG Policy • Data Protection Act 1998/Confidentiality Policy • Organisation Security Policy • Information Lifecycle Management (Records Management) Policy • Corporate Governance Policy	Policies set out scope and intent. The over-arching IG policy should reference the three supporting confidentiality, security and records management policies and might be where the organisation's intended IG Management Framework is documented.
Key Governance Bodies	IG Board/Forum/Steering Group (see below)	A group, or groups, with appropriate authority should have responsibility for the IG agenda. This might be one or more standalone groups or be part of an Integrated Governance Board or Risk Management group.
Resources	Details of key staff roles and dedicated budgets (see below)	The key staff involved in the IG agenda below those at Board or most senior levels should be identified with a description of their roles and responsibilities. Any dedicated budgets and high level plans for expenditure in-year should also be identified, including outsourcing to

		external resources or contractors.
Governance Framework	Details of how responsibility and accountability for IG is cascaded through the organisation. **(see criteria's 7 and 12)**	This should include staff contracts, contracts with third parties, Information Asset Owner (IAO) arrangements, Departmental leads on aspects of IG etc.
Training & Guidance **(see criteria 6)**	• Staff Code of Conduct **(see criteria's 5, 13 and 12)** • Training for all staff • Organisation Security Policy • Training for specialist IG roles	Staff need clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. The approach to ensuring that all staff receives training appropriate to their roles should be detailed.
Incident Management**(see criteria 11)**	Documented procedures and staff awareness	Clear guidance on incident management procedures should be documented and staff should be made aware of their existence, where to find them and how to implement them.

Information Governance Lead

3. A representative from the senior level of management (i.e. the Board or Senior Management Team) should be appointed as the overall IG lead and is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG. The key tasks of an IG lead include:

    a. developing and maintaining appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, e.g. an over arching high level strategy document supported by policies and procedures;

    b. ensuring that there is top level awareness and support for IG resourcing and implementation of improvements;

    c. providing direction in formulating, establishing and promoting IG policies;

    d. establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives;

    e. ensuring annual assessments and audits of IG policies and arrangements are carried out, documented and reported;

    f. ensuring that the annual assessment and improvement plans are prepared for approval by the senior level of management, e.g. the Board or senior management team, in a timely manner;

g. ensuring that the approach to information handling is communicated to all staff and made available to the public;

h. ensuring that appropriate training is made available to staff and completed as necessary to support their duties;

i. liaising with other committees, working groups and programme boards in order to promote and integrate IG standards;

j. monitoring information handling activities to ensure compliance with law and guidance;

k. providing a focal point for the resolution and/or discussion of IG issues.

Information Governance Board/Forum/Steering Group/Committee

4. Depending on organisational size and structure it may be appropriate to establish an IG forum, steering group or committee. This would comprise senior representatives from across the organisation and its professional disciplines to promote a holistic approach to IG and should be chaired by the IG Lead. It should also influence the integration and inclusion of IG standards with other governance, strategies, work programmes and projects, e.g. IT programmes.

5. The following are potential candidates for membership of the forum:

- IG Lead (Chair)
- SIRO
- Personal Data Guardian
- Clinical Director(s) or equivalent, e.g. medical and nursing directors
- Senior care professional(s), e.g. senior social worker
- Corporate Governance
- Corporate Communications
- Data Quality Leads
- Information Management
- Information Technology
- Human Resources/Personnel
- Governance Committee
- Freedom of Information Practitioner
- There may also be members that attend the forum on an ad hoc basis, e.g. to present a specific report or update.

6. There is no set format for IG and organisations will need to determine the arrangements that suit their requirements. Where it is felt that an IG Board/ Forum/Steering Group/Committee are too resource intensive it may be appropriate to add IG responsibilities to an existing governance Board or Risk Management Committee.

Information Governance Strategy, Policy and Associated Improvement Plans

7. The documentation required will consist of an over arching high level IG policy supported by corporate policies, strategies and plans covering the key areas of IG, for example:

- Confidentiality and Data Protection(DP);
- Information Security;
- Risk Management;
- Information lifecycle management including records management;
- Information Quality;
- Corporate Governance; and
- Freedom of Information (FOI).

Information Governance Policy

8. An IG policy is a statement of an organisation's intentions and approach to fulfilling its statutory and organisational responsibilities.

9. The key content of an IG policy should include:

- responsibilities for IG;
- use of information within the organisation;
- transfer of information in and out of the organisation;
- disclosure of information, whether person identifiable, sensitive, confidential or corporate;
- policy distribution and implementation;
- policy review and revision arrangements;
- IG related training and awareness for staff;
- monitoring of compliance with the policy and related procedures;
- approach to ensuring staff adhere to best practice guidance and code of conduct;
- disciplinary measures for failure to comply with the policy and related procedures.

10. Key areas addressing how information will be used within the organisation should include how the organisation will:

- proactively use information within the organisation, both for the care of service users and for service management as determined by law, statute and best practice;

- proactively use information with its partner organisations to support care as determined by law, statute and best practice;

- commit to making non-confidential information widely available in line with responsibilities under the Freedom of Information Act 2000;

- put in place effective arrangements to ensure the confidentiality, security and quality of personal and other sensitive information;

- ensure information within the organisation is of the highest quality in terms of completeness, accuracy, relevance, accessibility and timeliness.

Information Governance Strategy/Improvement Plan

11. An IG strategy or improvement plan may cover several years and should identify how the corresponding IG policy will be delivered.

12. Key elements of an IG strategy should include:

    - objectives and deliverables which should be:

        1. **Specific**: Define exactly what improvement is to be made.
        2. **Measurable**: Describe how it will be known that the improvement has been achieved.
        3. **Achievable**: Set realistic plans that can be achieved within the time constraints and resources available.
        4. **Relevant**: Relate the specific actions to ongoing improvement work.
        5. **Time-bound**: Set a date for completion.

    - resources to deliver the work programme;

    - risks and issues that may impact upon delivery;

    - description of impacts to existing systems and processes - including establishing links to risk management processes;

    - strategy ownership, approval and sponsorship;

    - the mechanism and frequency of reviews of the strategy;

    - how the strategy links to other organisational strategies, e.g. communications strategy, IM&T strategy.

Reporting

13. The senior level of management should receive periodic assurance that management and accountability arrangements are adequate, and be informed in a timely manner of future changes in the IG agenda. These need to be considered and addressed. The IG Lead must ensure there are adequate arrangements in place for:

    - reporting IG events or incidents e.g. information quality failures, actual and potential breaches of confidentiality or information security;

    - analysing, investigating and upward reporting of events / incidents and any recommendations for remedial action;

- IG progress reports;
- reporting annual IG assessment and improvement plans;
- communicating IG developments and standards to appropriate forum and staff.
- continuing to demonstrate compliance with the key IG standards, Controls Assurance Standards and ensuring plans are in place to progress beyond the minimum where it has been achieved;
- mandating all staff to complete basic IG training(see criteria 6);
- continuing to report on the management of the information risks in statements of internal controls and to include details of data loss and confidentiality breach incidents in annual reports;
- ensuring an IG audit is included within each organisation's auditors work plan.

Evidence Demonstrating Compliance

For minimal compliance Organisations should evidence that:

- the Information Governance Management Framework has been documented and there are comprehensive IG policies that cover the breadth of the IG agenda and they have been approved by the senior level of management in the organisation.

In order to move to moderate and then substantive compliance Organisations would be required to evidence that:

- the Information Governance Management Framework has been signed off by the Board or equivalent senior management tier and the key governance bodies have been established and are active. The IG policies have been communicated to staff and there are strategies and/or improvement plans in place to deliver IG improvements.

- in-year reports and briefings on IG arrangements, implementation of strategies and/or improvement plans are provided to and considered by the senior level of management in the organisation, who annually approve any necessary improvements to existing arrangements.

Links With Other Standards

Governance

ICT Management

Department of Health Information Governance Toolkit Reference - 13-101 and 13-105

Criterion 2

An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy

INFORMATION

Criterion Description

Organisations should ensure that appropriately senior individuals are allocated responsibility for owning information risk. In HSC organisations this role is referred to as the SIRO, who should be an Executive Director or other senior member of the Board (or equivalent), e.g. senior management committee. SIROs should be familiar with information risks and the organisation's response to risk to ensure they can provide the necessary input and support to the Board and to the Accounting Officer.

Source

- Cabinet Office: Data Handling Procedures in Government: Final Report June 2008 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60966/final-report.pdf

- International Standards Organisation BSO ISO/IEC 27000 Series of Information Security Standards http://www.27000.org/

- DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information January 2012 https://www.health-ni.gov.uk/publications/code-practice-protecting-confidentiality-service-user-information
- DHSSPS AMCC 2649 Letter dated 22/09/10 to Chief Executives of HSC Organisations – Senior Information Risk Owner and Information Asset Owner from A McCormick

Guidance

Information Risk - Responsibilities and Accountability

1. Information risk should be managed in a robust way within work areas and not be seen as something that is the sole responsibility of IT or IG staff. Assurances need to be provided in a consistent manner and can be achieved through the development of an IG framework.

2. This structured approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff. The establishment of the role of SIRO is one of several measures to strengthen controls around information security outlined in the Cabinet Office review and report on data handling in 2008.

Accountability and Performance

3. Senior level ownership of information risk is a key factor in successfully raising the profile of information risks and to embedding information risk management into the overall risk management culture of the organisation. Senior leadership demonstrates the importance of the issue and is critical in obtaining the resources and commitment necessary to ensuring information security remains high on the agenda of the Board (or equivalent), e.g. senior management group/committee.

The Role of the Accounting Officer

4. In the HSC, the Chief Executive is the Accounting Officer of the organisation and has overall accountability and responsibility for Information Governance. S/he is required to provide assurance, through the Statement of Internal Controls, that all risks to the organisation, including those relating to information, are effectively managed and mitigated.

The Role of the Senior Information Risk Owner

5. The SIRO should be an Executive Director or other senior member of the Board familiar with information risks and is the focus for management of information risk at Board Level but should not be the Personal Data Guardian as the SIRO should be part of the organisation's management hierarchy rather than being in an advisory role.

6. The SIRO will be expected to understand how the strategic business goals of the organisation may be impacted by information risks and it may therefore be logical for this role to be assigned to a Board member already leading on risk management or IG.

7. The SIRO will act as an advocate for information risk on the Board and in internal discussions, and will provide written advice to the Accounting Officer on the content of the annual Statement of Internal Control (SIC) in regard to information risk.

8. The SIRO will provide an essential role in ensuring that identified information security risks are followed up and incidents managed and should have ownership of the Information Risk Policy and associated risk management Strategy and processes. He/she will provide leadership and guidance to a number of IAOs.

9. The key responsibilities of the SIRO are to:

    a. oversee the development of an Information Risk Policy, and implementing the policy within the existing IG Framework;

    b. take ownership of the risk assessment process for information risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control;

c. review and agree action in respect of identified information risks;

d. ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff;

e. provide a focal point for the resolution and/or discussion of information risk issues;

f. ensure the Board is adequately briefed on information risk issues.

Training

10. The SIRO will be required to successfully complete strategic information risk management training followed by annual refresher training.

The Role of Information Asset Owners

11. For information risk, IAOs are directly accountable to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets.

12. It is particularly important that each IAO (or equivalent) should be aware of what information is held and the nature of and justification for information flows to and from the assets for which they are responsible.

13. The role of the IAO is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. As a result they should be able to understand and address risks to the information and to ensure that information is fully used within the law for the public good. The IAO will also be responsible for providing or informing regular written reports to the SIRO (or equivalent), a minimum of annually on the assurance and usage of their asset.

14. It is important that "ownership" of Information Assets is linked to a post, rather than a named individual, to ensure that responsibilities for the asset are passed on, should the individual leave the organisation or change jobs within it.

Information Assets (IAs)

15. IAs are identifiable and definable assets owned or contracted by an organisation which are 'valuable' to the business of that organisation. IAs will likely include the computer systems and network hardware, software and supporting utilities and staff that are required to achieve processing of this data, though IAs should not be seen as simply technical. There are many categories of IA including:

a. **Information**. Databases, system documents and procedures, archive media/data, paper records etc.

b. **Software**. Application programs, system, development tools and utilities.

c. **Physical**. Infrastructure, equipment, furniture and accommodation used for data processing.

d. **Services**. Computing and communications, heating, lighting, power, air-conditioning used for data processing.

e. **People**. Their qualifications, skills and experience in use of information systems.

f. **Intangibles**. For example, public confidence in the organisation's ability to ensure the Confidentiality, Integrity and Availability of personal data.

16. As these categories suggest, IAs are not necessarily tangible objects; business processes and activities, applications and data should all be considered as IAs, however, their degree of importance to the organisation may vary.

Information Asset Register

17. It is vital that all organisations establish programmes that ensure their IAs are identified and assigned to an IAO (or equivalent). The SIRO (or equivalent), should oversee a review of the organisation's asset register to ensure it is complete and robust.

18. IAs should be documented in a register. In practice, a number of asset registers may exist (e.g. departmental), and many will be ad hoc. In order to establish corporate coherence it should be possible for a single asset register to be created for the organisation. As a priority, it is essential that all critical IAs are identified and included in this asset register, together with details of business criticality, the IAO (or equivalent), and risk reviews carried out. To improve its usability and maintainability, the Information Asset register may be organised by service, rather than location.

19. The best type of IA register will link all the categories listed above. It makes good risk management sense to group all of the components that relate to the same information asset or business process together. For example, you might put an IT system, its system documentation, its physical location, the data held within it and the skills of staff who administer it into one IA category.

20. Details of a business process, such as a particular employment position, should be seen as an asset, with job description, location in organisational structure, qualification / experience necessary for the position, employee development plan, etc all linked to the business process.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- there is a SIRO with an effective support infrastructure in place and adequate information risk skills, knowledge and experience to successfully co-ordinate and implement information risk management.

In order to move to moderate and then substantive compliance Organisations would be required to evidence that:

- the SIRO and supporting Information Risk Management leads (IAOs and supporting staff) are appropriately trained and conduct regular risk reviews for all key assets.

- the arrangements for information risk management are regularly reviewed to ensure they remain current and effective. The SIRO successfully completes strategic information risk management training at least annually.

Examples of evidence include:

- named individuals' job descriptions;
- Asset Register;
- risk reviews;
- training attendance lists;
- training materials;
- attendance/qualification certificates;
- confidentiality strategy;
- report for senior management;
- Minutes of meetings.

These are only examples and it is the responsibility of each organisation to determine how they evidence compliance.

Links with other standards

Governance

Risk Management

Department of Health Information Governance Toolkit Reference - 13-307

Criterion 3

Documented and implemented procedures are in place for the effective management of corporate records

INFORMATION

Criterion Description

Effective records management requires that an organisation is able to identify and retrieve information when and where it is needed. The organisation must have records management procedures in place that cover the creation, filing, location, retrieval, appraisal, archive and destruction of records in accordance with Good Management Good Records (GMGR), and other relevant guidance and legislation.

Source

- Great Britain (1923) The Public Records Act (NI) 1923 The Stationery Office, London http://www.legislation.gov.uk/apni/1923/20
- Great Britain (1925) Disposal of Documents Order, 1925 http://www.proni.gov.uk/1925_disposal_of_documents_order.pdf
- Great Britain (2000) The Freedom of Information (FOI) Act 2000 The Stationery Office, London http://www.legislation.gov.uk/ukpga/2000/36/contents
- Great Britain (2004) Environmental Information Regulations 2004 The Stationery Office, London http://www.legislation.gov.uk/uksi/2004/3391/contents/made
- Great Britain (2004)The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 The Stationery Office, London http://www.legislation.gov.uk/uksi/2004/3244/contents/made
- Secretary of State for Constitutional Affairs' Code of Practice on the discharge of public authorities' functions under Part I of the Freedom of Information Act 2000, published 2004
- DHSSPS Guidelines for Managing Records in Health and Personal Social Services Organisations in Northern Ireland – Good Management Good Records November 2011 https://www.health-ni.gov.uk/topics/good-management-good-records
- Great Britain. Lord Chancellors Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000. (2009) London: The Lord Chancellor's Department. http://www.nationalarchives.gov.uk/information-management/projects-and-work/records-management-code.htm
- International Standard Organisation International Standard ISO 15489 1:2001(E) Information and Documentation – Records Management http://www.iso.org/iso/catalogue_detail?csnumber=31908

- Public Record Office Northern Ireland (PRONI) Guidelines on Information Audits and Disposal Schedules for NI Public Auth
  https://www.nidirect.gov.uk/publications/guidelines-information-audits-and-disposal-schedules-northern-ireland-public

- Public Record Office Northern Ireland (PRONI) – Northern Ireland Records Management Standard https://www.nidirect.gov.uk/articles/records-management-public-bodies

GUIDANCE

Corporate Records Management

1. The records management function should be recognised as a specific corporate responsibility for all HSC organisations and departments. It should provide a managerial focus for records of all types in all formats, including electronic records, throughout their life cycle, from planning and creation through to ultimate disposal. It should have clearly defined responsibilities and objectives, and adequate resources to achieve them.

2. In the context of Corporate Information Assurance, corporate information refers to information generated and received by an organisation other than clinical/care (or service user) information. The term describes the records generated by an organisation's business activities, and therefore will include records from the following (and other) areas of the organisation:

    - Estates/Engineering;
    - Financial;
    - Information Management & Technology (IM&T);
    - Personnel/Human Resources;
    - Risk Management and Governance;
    - Purchasing/Supplies.

3. This requirement aims to ensure that corporate records, whether paper or electronic, are accessible and retrievable when and where required. It is not only concerned with corporate records that are part of a formal document and record management system, but includes any records on network drives and in shared folders. Emails and attachments, and web pages on internet and intranet sites that are considered corporate records, must also be included within the procedures.

4. When handling any type of record, it is important to make the distinction between a record and a document. In the context of this criterion, a document becomes a record when it has been finalised and become part of an organisation's corporate information. At this point, the record should not be amended and should only be held in the corporate system, for example, a registered organisational file, approved EDRMS system, the network drive, shared folder, and not on a local drive on a PC or laptop.
   ****This requirement should be reviewed in conjunction with criteria 10, as organisations may need to undertake a corporate records audit prior to**

developing record management procedures to ensure they are aware of all the records held, their location and format, which should in turn inform the decisions made to utilise effective records management systems.**

Records Management – Procedures

5. Organisations should ensure they have documented corporate records management procedures in place which are communicated to all staff and set out following areas:

a. **Creation**

i. Record creation is one of the most important processes in records management and organisations should aim to create good records in an effective system. However, creating a record is not enough unless the record is then captured or filed into a filing system created and managed by the organisation.

ii. It is important that records are kept in their context and the best way to achieve this is to file or classify them. Records cannot be tracked or used efficiently if they are not classified or if they are classified inappropriately. Records captured or filed in a corporate filing system will possess some of the necessary characteristics to be regarded as authentic and reliable. Whatever the format of the records, they should be saved into a proper records management system.

iii. A common format for the creation of records will ensure that those responsible for record retrieval are able to locate records more easily.

iv. The documented procedures should inform staff how to create corporate records in a common format, including:

- the difference between a document and a record;
- the referencing to be applied to new records;
- the version control standards to be followed;
- the agreed naming conventions in use in the organisation;
- where an original record should be filed;
- how to apply a protective mark to a record, if appropriate.

b. **Naming**

i. Naming conventions should:

- give a unique name to each record;
- give a meaningful name which closely reflects the records contents;
- express elements of the name in a structured and predictable order;
- locate the most specific information at the beginning of the name and the most general at the end;

- give a similarly structured and worded name to records which are linked (for example, an earlier and a later version).

c. **Filing structure**

i. A clear and logical filing structure that aids retrieval of records should be used. Ideally, the filing structure should reflect the way in which paper corporate records are filed to ensure consistency. However, if it is not possible to do this, the names allocated to files and folders should allow intuitive filing. Filing of the primary corporate record to local drives on PCs and laptops should be strongly discouraged.

ii. The agreed filing structure should also help with the management of the retention and disposal of records – see **paragraph 5f** below.

d. **File/Folder Referencing**

i. A referencing system should be used that meets the organisation's business needs, and can be easily understood by staff members that create documents and records. Several types of referencing can be used, for example, alphanumeric; alphabetical; numeric; keyword. The most common of these is alphanumeric, as it allows letters to be allocated for a business activity, for example, HR for Human Resources, followed by a unique number for each record or document created by the HR function.

ii. It may be more feasible in some circumstances to give a unique reference to the file or folder in which the record is kept and identify the record by reference to date and format.

e. **Tracking and Tracing**

i. There should be tracking and tracing procedures in place that enable the movement and location of records to be controlled and provide an auditable trail of record transactions. The process need not be a complicated one, for example, a tracking procedure could comprise of a book that staff members sign when a corporate record is physically removed from or returned to its usual place of storage (not when a record is simply removed from a filing cabinet by a member of staff from that department as part of their everyday duties).

Tracking mechanisms to be used should include:

- the item reference number or identifier;
- a description of the item (for example the file title);

- the person, position or operational area having possession of the item;
- the date of movement.

Systems for monitoring the physical movement of records, for example:

- location cards;
- index cards;
- docket books;
- diary cards;
- transfer or transit slips;
- bar-coding;
- computer databases (electronic document management systems);
- regular record audits.

ii. The system adopted should maintain control of the issue of records, the transfer of records between persons or operational areas, and return of records to their home location for storage. The simple marking of file jackets to indicate to whom the file is being sent is not in itself a sufficient safeguard against files going astray.

f. **Retention and disposal**

i. Retention/disposal procedures must be based on Good Management Good Records which has been approved by the Northern Ireland Assembly and endorsed by the Chief Executives of all HSC organisations.

ii. Records selected by PRONI for archival preservation and no longer in regular use by the organisation should be transferred to PRONI in accordance with the guidance in GMGR. Non-active records should be transferred no later than 20 years from closure of the record, as required by the Public Records Act (NI) Act 1923.

iii. When developing or purchasing a records management system, organisations should consider how retention/disposal periods will work or can be factored into the system. For paper corporate records, this may be using clearly marked labels on each folder to state the minimum retention period, and a log kept so that records can be easily appraised.

iv. Electronic document management systems may have the functionality built within them to set the disposal period for a record based on certain defined rules.

v. Methods used throughout the destruction process must provide adequate safeguards against the accidental loss or disclosure of the contents of the records. If contractors are used, they should be required to sign confidentiality

undertakings and to produce written certification as proof of destruction.

vi. A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved, so that the organisation is aware of those records that have been destroyed and are therefore no longer available.

Records Management Systems

6. Records must be maintained in a system that ensures they are properly stored and protected throughout their life cycle, this includes any electronic records that are migrated across to new systems. Therefore, before procuring new systems or putting new processes in place, organisations should take into account the need to keep up with technological progress (e.g. new hardware, software updates) to ensure that records remain accessible and retrievable when required.

   A records management system should ensure:

   a. there are accurate audit trails of when records are created (i.e. the date that a document becomes a formal corporate record), accessed (e.g. a sign-out book, or automatic date modified note against file name for electronic records) and disposed of;

   b. records are grouped in a logical structure to enable the quick and efficient filing and retrieval of information when required and enable implementation of authorised disposal arrangements, i.e. archiving or destruction;

   c. there are suitable storage areas so that records, whether physical or electronic, remain accessible and usable throughout their life cycle;

   d. access to records is controlled through a variety of security measures, for example, authorised access to storage and filing areas, lockable storage areas, user verification, password protection and access monitoring;

   e. issue from and return to storage areas on site or to authorised off-site facilities is documented;

   f. technological upgrades are supported so that records remain accessible and usable throughout their life cycle;

   g. cross-referencing of electronic records to their paper counterparts is permitted (where dual systems are maintained).

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- there are documented and approved corporate records management procedures which incorporate the creation, filing, tracking, appraisal, retention and destruction of records.

In order to move to moderate and then substantive compliance Organisations would be required to evidence that:

- the procedures have been implemented. All staff members have access to and have been effectively informed of the procedures.

- the effectiveness of the implemented procedures is regularly reviewed. All staff members that create electronic corporate records comply with the procedures.

Examples of evidence include:

- named individuals' job descriptions;
- procedures
- communications with staff;
- tracking systems
- report for senior management;
- minutes of meetings.

These are only examples and it is the responsibility of each organisation to determine how they evidence compliance.

Links with other standards

Department of Health Information Governance Toolkit Reference - 13-601

Criterion 4

Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information (FOI) Act 2000 and Environmental Information Regulations 2004 (EIR)

INFORMATION

Criterion Description

Public Authorities since January 2005 have a statutory requirement to comply with the Freedom of Information Act (FOIA) 2000 and Environmental Information Regulations 2004 (EIR)**.** Compliance with these Acts includes providing information upon request within the terms of FOI and EIR as well as providing and maintaining a publicly accessible Publication Scheme, which should proactively make available information created by the Public authority.

Source

- Great Britain (2000) The Freedom of Information (FOI) Act 2000 The Stationery Office, London http://www.legislation.gov.uk/ukpga/2000/36/contents

- Great Britain (2004) Environmental Information Regulations 2004 The Stationery Office, London http://www.legislation.gov.uk/uksi/2004/3391/contents/made

- Great Britain (2004)The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 The Stationery Office, London http://www.legislation.gov.uk/uksi/2004/3244/contents/made

- Secretary of State for Constitutional Affairs' Code of Practice on the Discharge of Public Authorities' Functions under Part I of the Freedom of Information Act 2000 November 2004 http://www.justice.gov.uk/downloads/information-access-rights/foi/foi-section45-code-of-practice.pdf

- DHSSPS Guidelines for Managing Records in Health and Personal Social Services Organisations in Northern Ireland – Good Management Good Records November 2011 https://www.health-ni.gov.uk/topics/good-management-good-records

- Information Commissioner' Office Definition documents and template guides to information http://www.ico.org.uk/for_organisations/freedom_of_information/definition_documents

- Information Commissioner's Office Freedom of Information Act Model Publication Scheme Version 2 January 2009 http://www.ico.org.uk/upload/documents/library/freedom_of_information/practical_application/usingthedefinitiondocuments.pdf

GUIDANCE

Compliance with the Freedom of Information Act 2000 and Environmental Information Regulations 2004

1. The Freedom of Information Act 2000 (FOIA) and Environmental Information regulations 2004 (EIRs) came into force at the beginning of 2005 and provide public access to information held by public authorities including government departments, local authorities, the HSC, state schools and police forces. The FOIA requires public authorities to have an approved publication scheme in place providing a way to proactively publish information as part of its normal business activities.

Responsibilities for Freedom of Information Act (FOIA) and Environmental Information Regulations (EIR) Compliance

2. The Chief Executive has the ultimate responsibility for their Public Authority's compliance with both FOIA and EIR and should ensure that responsibility for reporting issues to the Board (or equivalent) is delegated to an appropriate Director (or equivalent) to act as FOI and EIR lead.

Freedom of Information and Environmental Information Regulation Lead

3. The senior management level lead should ensure organisational procedures and processes are in place to comply with the FOIA and EIR. The key responsibilities are to:

    - ensure that the organisation complies with all aspects of both the FOIA and EIR, associated Codes of Practice and related provisions in particular for contracting and procurement, minutes of meetings etc;
    - provide reports to the Board (or equivalent) highlighting resource, performance and compliance issues;
    - draft and/or maintain the currency of the organisation's policy;
    - ensure that all staff are aware of their personal responsibilities for compliance with both the FOIA and EIR and adhere to organisational policies and procedures;
    - ensure training and written procedures are widely disseminated and available to all staff;
    - ensure the general public has access to information about their rights under the FOIA and EIR;
    - establish appropriate arrangements to deal with appeals and investigations into complaints about decisions and response times;

- liaise and work with other functions responsible for information handling activities, for example the Personal Data Guardian, data protection and information security staff;

- contribute to, or liaise with, external FOI networks or groups to keep updated on 'round robin requests' (see **paragraph 36**).

Information Manager/Staff

4. An individual should be nominated to manage the FOI and EIR process and support staff, and routinely report to the FOI and EIR Lead and Board (or equivalent).

All Directors and Heads of Service (and equivalents)

5. All corporate information, for example contracts and commercially sensitive information should be created with the awareness that a request for this information may be received and information which is not exempt under the FOIA or an exception under EIR must be disclosed to comply with the FOIA or EIR. Senior members of staff should therefore ensure that they (and their staff) receive adequate training to ensure they are able to adhere to policies, procedures and guidance.

All Staff Members

6. All staff should be made aware of their own personal responsibilities for the creation of records including emails which may be subject to and disclosed in response to an FOI or EIR request. In addition, each member of staff should be aware of the organisation’s process for dealing with a request which is received by them, for example who to contact and the urgency for doing so due to the strict time limits which the law applies.

Information Governance Committee/Group

7. The IG Committee/Group should receive regular FOI/EIR performance reports which highlight:

- numbers of requests received;

- numbers responded to within the 20 working day limit and the reasons for any exceeding the statutory deadline;

- the justification for the application of any exemptions or exceptions;

- details of any complaints made about any response or the process itself;

- details of any requests that have been escalated to the Information Commissioner's Office by the applicant.

8. Based on these reports the IG Committee/Group should agree any necessary improvement plans recommendations for improvements, for example identify additional resources if there is continued failure to meet statutory deadlines, increasing staff awareness through additional training or guidance materials

Staff Training and Awareness

9. Comprehensive training should be provided for staff working in areas where requests are managed. The training should cover:

    - recognising and responding to a request for information;
    - developing and maintaining a Publication Scheme;
    - records management;
    - exemptions and exceptions – public interest and absolute exemptions;
    - complaints / enforcement;
    - the interface between freedom of information and data protection;
    - vexatious/repeated requests;
    - fees.

10. Support staff who may assist with locating and collating information should receive basic training in FOI and EIR issues.

Publication Schemes

11. The FOIA requires every public authority to adopt and maintain a publication scheme which has been approved by the Information Commissioner, and to publish information in accordance with the scheme.

12. The publication scheme must set out the following:

    - the classes of information published, or intended to be published;
    - the manner in which publication is, or is intended to be made;
    - a schedule of any fees charged for access to information which is made proactively available.

13. In January 2009 the Information Commissioner published a single approved model publication scheme which must be adopted by all public authorities. Organisations should adopt the approved scheme by placing a link to it on their website or otherwise making it available and should also:

- use the appropriate definition document (see **paragraph 14** below) and any previous publication scheme to identify the information held by the organisation that should be published;

- produce a **guide to information**, (or ensure that an existing website meets this need) that specifies the particular information the organisation publishes, how it will be published and what charge if any is to be made;

- ensure that members of the public can easily obtain the information.

14. The Information Commissioner's Office has produced a number of definition documents for use by central and local government, education, health, and the police which set out the types of information they would expect public authorities to publish and list in their guide to information.

15. Organisations should maintain a log of requests, referred to as a disclosure log, with a view to making this publicly available. A publicly available disclosure log may help to reduce the numbers of similar requests (for example MRSA rates, bed numbers) an organisation receives as the information will be easily accessible and a separate request may therefore be unnecessary.

Provision of Advice and Assistance

16. The public may or may not be aware that information is available to them under the FOIA 2000 (or EIR 2004). All organisations should assist in the communication of this fact by widely publicising the way in which the public may gain access to information covered by the Act. Organisations should have materials to support communications about FOI applications, supported by FOI request handling procedures.

17. Organisations also have an obligation to assist the public with making a request, for example if a request is made verbally by someone who is unable to read or write. In this case, an organisation should assist the applicant to write down their request and encourage him/her to verify with a friend or family member that the written request is in fact what is required. A similar approach can be taken with applicants who may not speak English and require assistance to write down their request.

18. It is particularly important that clinical / care staff members, and others dealing directly with service users and the public, are fully informed of the duty to provide advice and assistance.

19. An organisation should develop clear, publicly available, request handling procedures that are formally documented. The procedures should address the making of a FOI application and describe how such an application will be handled by the organisation. They should also address issues such as refusal of requests, the organisation's duty to provide a notice if a request is refused

and provide a route for the applicant to make a complaint or lodge an appeal with the Information Commissioner.

Provision of Advice and Assistance

20. The FOIA 2000 confers two rights on the general public:

- the right to be informed whether a public body holds certain information;
- the right to obtain a copy of that information.

21. All organisations should aim to ensure that:

- the majority of information is made available through the organisation's guide to information;
- other information is readily available on request;
- if the information requested is assessed to be currently subject to an exemption, or exception, the organisation should provide a process to enable a judgement to be made as to whether the information can be released.

22. Where possible the information should be supplied in the format requested by the applicant. However, requests can be met by providing a copy of the original document, a digest/summary of the original or even by allowing the applicant to visit the organisation to read the document(s).

23. Requests for information should be met within 20 working days of receipt of the request or, where a fee is charged, within 20 working days of receipt of that fee. Additionally, if the organisation requires further clarification to enable it to identify the information requested, the 20 working days will not begin to run until the applicant has provided that clarification.

24. Responding to a request within the limits requires that the organisation can quickly locate and retrieve information. This Requirement is therefore dependent on work carried out to meet Corporate Information Assurance **criteria 3** related to the audit of information held by an organisation, and Corporate Information Assurance **criteria 10** regarding the effective management of corporate records.

Fees

25. Organisations are permitted to charge reasonable fees to meet some of the cost of providing information and may charge for reasonably incurred costs to:

- inform the applicant whether the organisation holds the information;
- communicate the information to the applicant.

26. The fee may include:

- the cost of putting the information into the applicant's requested format, e.g. CD, audio tape;
- photocopying and printing costs (set at no more than 10 pence per page);
- postage or other transmission costs.

27. Additionally, organisations may not charge for putting the information into another format if they are already under a duty to make information accessible under other legislation, e.g. the Disability Discrimination Act 1995. Furthermore, if organisations have an internal translation service, it would not be reasonable to charge a fee for translation into a language provided by members of that service.

Complex or Costly Requests

28. There may be a few cases where the costs of meeting a request would exceed the appropriate limit, set at £450. If this is the case, organisations may be exempt from answering the request.

29. The limit is applied first to the organisation's duty to confirm or deny that it holds the information and then to its duty to supply the information. Therefore, if it would cost more than £450 to confirm or deny then there is no duty to do so.

30. Organisations are permitted to estimate whether the cost of meeting a particular request would exceed the £450 limit. To do this they should take into account the costs of employing staff to:

- find out whether the information is held;
- locate and retrieve the information;
- extract the information (including editing and redacting).

31. To estimate these staff costs organisations should use an hourly rate of £25 per person per hour. In making this estimation, no other costs may be taken into account.

Exempted Information

32. Organisations may receive requests for information that are judged to be exempt (exceptions under EIR) from release; however, the relevant information should be kept under review, as it may be possible to release it in the future. This may include information provided by third parties given with the expectation that it would be held in confidence, for example, tenders for contracts before the contract has been awarded. Once the contract has been awarded, it might be possible to release the successful and unsuccessful tenders if a request is made.

Complaints and Appeals

33. The Environmental Information Regulations 2004 (EIR) is the only legislation that requires the Information Commissioner to have a review procedure, however this procedure will also be adopted for use in relation to complaints made to the Information Commissioner regarding request for information made under the Freedom of Information Act 2000 (FOIA) and indeed both the Code of Practice made under section 45 of the FOIA 2000 and the Information Commissioner's Office recommend it is good practice to have one. Section 17(7) of the FOIA and regulation 14(5) of the EIR provides that, in a refusal notice, an authority must give details of any review procedures, as well as details of the right of appeal to the Information Commissioner.

34. Organisations should assign responsibility for dealing with any complaints and appeals, e.g. initial complaints about the organisation's FOI procedures and appeals against decisions not to supply exempt information. Staff that manage FOI and EIR requests should be alert to the possibility that a request may have been sent to a number of organisations - 'round robin requests' - and there should be a documented procedure for alerting HSC IM leads so that they can provide coordination and support. HSC IM Leads should in turn alert the Department of Health.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- there are documented procedures for FOIA 2000 and EIR 2004 compliance, which set out clear responsibilities for responding to information requests efficiently and in accordance with the law. The ICO model publication scheme has been adopted and a guide to information has been communicated to, and is accessible by, members of the public.

In order to move to moderate and then substantive compliance Organisations would be required to evidence that:

- all staff members are aware of their responsibility to support requests for information, and are aware of where in the organisation such requests should be directed. Front-line staff members are provided with more detailed guidance about the procedure to follow. Staff in areas where requests are ultimately managed are provided with comprehensive training.

- the procedures for FOIA and EIR compliance are regularly reviewed and issues of non compliance, complaints and appeals are appropriately dealt with. Where necessary, additional measures have been implemented to assess and improve performance in meeting the statutory timeframes.

Examples of evidence include:

- named individuals' job descriptions;
- documented policies and strategies;
- guidance and awareness materials;
- links to publication scheme and a guide to information on the organisations website;
- posters;
- training materials;
- training attendance records;
- report for senior management;
- minutes of meetings.

These are only examples and it is the responsibility of each organisation to determine how they evidence compliance.

Links with other standards

Governance

Department of Health Information Governance Toolkit Reference - 13-603

Criterion 5

Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users and staff

INFORMATION

Criterion Description

All organisations have a legal and ethical duty to keep all personal information secure and to respect confidentiality when personal information is held in confidence. This requires all staff to be aware of their responsibilities set out within a code of conduct or equivalent guidance, which is supported by relevant policies and appropriate procedures.

Source

- Great Britain Department of Health 1997 The Caldicott Report, Review of Patient Identifiable Information Recommendation 2 http://www.google.co.uk/url?url=http://webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/%40dh/%40en/documents/digitalasset/dh_4068404.pdf&rct=j&frm=1&q=&esrc=s&sa=U&ei=xJHkVOCsFpPqaJPwgYgF&ved=0CBQQFjAA&usg=AFQjCNGlrEb5TnxzJPg_5AIzG78tp8Cl-w

- Great Britain (1998) the Data Protection Act 1998 The Stationery Office, London http://www.legislation.gov.uk/ukpga/1998/29/contents

- Great Britain (1998) the Human Rights Act 1998 The Stationary Office London http://www.legislation.gov.uk/ukpga/1998/42/contents

- Great Britain Department of Health Health service circular 1999/012 Caldicott Guardians http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Publicationsandstatistics/Lettersandcirculars/Healthservicecirculars/DH_4004311

- DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information January 2012 https://www.health-ni.gov.uk/publications/code-practice-protecting-confidentiality-service-user-information
- Great Britain Department of Health The Caldicott Guardian Manual 2010 http://systems.hscic.gov.uk/infogov/links/2010cgmanual.pdf
-

- DHSSPS The Quality Standards for Health and Social Care Supporting Good Governance and Best Practice in the HSC, March 2006

- Northern Ireland Social Care Council Standards of Conduct and Practice http://niscc.info/news/27-whats-new-in-the-niscc-standards-focus-on-the-consultation-process

- General Medical Council, Guidance for Doctors Confidentiality October 2009 http://www.gmc-uk.org/guidance/news_consultation/25893.asp

- Nursing and Midwifery Council The Code, Standards of Conduct performance and ethics for nurses and midwives May 2008 http://www.nmc-uk.org/Nurses-and-midwives/Standards-and-guidance1/The-code/The-code-in-full/

- UK Council for Health Informatics Professionals Code of Conduct http://www.ukchip.org/?q=page/UKCHIP-Code-Conduct

- Information Commissioner's Office Information Commissioner's guidance about the Issue of Monetary Penalties prepared and issued under section 55C(1) of the Data Protection Act 1998 The Stationary Office London ISBN 9780108511240 http://www.official-documents.gov.uk/document/other/9780108511240/9780108511240.asp

- International Standard Organisation International Standard ISO 15489 1:2001(E) Information and Documentation – Records Management http://www.iso.org/iso/catalogue_detail?csnumber=31908

GUIDANCE

Information Governance/Confidentiality Code of Conduct

1. The obligation to keep personal information secure and to respect confidentiality stems from common law, data protection and human rights legislation and applies to all organisations. Staff working for and on behalf of the organisation must also meet these legal requirements and may be bound by professional obligations, employment contracts or other contractual measures. It is essential therefore, that organisations ensure their staff understand what they need to do to keep information safe and secure.

2. Organisations should also be aware of the principle of vicarious liability, which applies where a negligent act or omission (e.g. loss of personal data) by an employee is so closely connected with the performance of their employment that it would be fair to place the liability on the employer. A situation such as this could arise for example, where there has been a data loss and an investigation finds that the organisation has failed to inform a member of staff of the procedure or processes required to keep personal information secure and confidential.

Content of Guidance for Staff

3. To ensure staff members are effectively informed of what is required of them, the organisation should ensure they have access to a code of conduct or equivalent guidance that identifies legal requirements and best practice.

4. Where required the code should be tailored to the needs of different staff groups. This requires in all cases that a thorough assessment of staff needs has been carried out to determine whether such guidance is required, e.g. for staff working with particularly sensitive information or those who have little access to confidential information.

5. As a minimum, the code should inform staff about:

   - **the legal framework and the circumstances under which confidential information can be disclosed.** Guidance includes the Code of Practice on Protecting the Confidentiality of Service User Information, and the Caldicott Principles. Care professionals must also comply with the codes of practice of their respective professions. Although these guidelines may not be suited for direct local use they provide a basis for local codes which can focus on particular work areas or staff groups. The Caldicott Principles are reproduced below. More detail on content can be found in criteria 12 in respect of consent and other lawful reasons for information sharing.

   - **the systems and processes for protecting personal information.** This will include any safe haven procedures, e.g. for answering telephone queries or receiving confidential faxes, any information sharing protocols agreed with external organisations, encryption requirements for mobile devices etc. See criteria 16 for detailed guidance on secure transfers of personal information.

   - **who to approach within the organisation for assistance and advice on disclosure issues.** Although there may be a range of individuals who can assist with difficult issues – IG leads, Personal Data Guardians, SIROs, DP leads etc. – it is important that each organisation provides clear signposts to its staff.

   - **possible sanctions for breach of confidentiality or data loss.** The organisation should ensure that all staff members are aware of the possible disciplinary sanctions for failure to comply with their responsibilities, e.g. deliberately looking at records without authority; discussion of personal details in inappropriate venues; transferring personal information electronically without encrypting it, etc. Sanctions can include disciplinary action, ending a contract, dismissal, or bringing criminal charges. Since April 2010, the Information Commissioner's Office (ICO) may order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act 1998. The ICO has produced statutory guidance about how it proposes to use this power.

6. The organisation should ensure staff are effectively informed about the code through awareness sessions, team meetings, briefing notes or a combination of these. The code must be accessible so it needs to be readily available e.g.

published on the Intranet or providing staff with their own copy. Understanding what is required should be supported through staff training.

The Caldicott Principles

7. The Principles were devised by the Caldicott Committee, which reported in 1997 following a review of patient-identifiable information. They represent best practice for using and sharing identifiable personal information and should be applied whenever a disclosure of personal information is being considered:

    - Principle 1: Justify the purpose for using the information
    - Principle 2: Only use it when absolutely necessary
    - Principle 3: Use the minimum that is required
    - Principle 4: Access should be on a strict need to know basis
    - Principle 5: Everyone must understand their responsibilities
    - Principle 6: Understand and comply with the law

Evidence Demonstrating Compliance

For minimal compliance Organisations should evidence that:

- there is documented guidance for staff on keeping personal information secure and on respecting the confidentiality of service users that has been approved by senior management or committee.

In order to move to moderate and then substantive compliance Organisations would be required to evidence that:

- the documented and approved staff guidance has been made available at appropriate points in the organisation and all staff members have been effectively informed about it and the need for compliance. Where appropriate the guidance is tailored to particular staff groups or work areas.

- Staff compliance with the guidance, on keeping personal information secure and on respecting the confidentiality of service users, is monitored and assured.

Examples of evidence include:

- named individuals' job descriptions;
- a copy of the guidance;
- staff induction training materials;
- report for senior management;
- minutes of meetings.

These are only examples and it is the responsibility of each organisation to determine how they evidence compliance.

Links with other standards

Governance

ICT Management

Department of Health Information Governance Toolkit Reference - 13-201

Criterion 6

Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained

INFORMATION

Criterion Description

To ensure organisational compliance with the law and central guidelines relating to IG, staff must receive appropriate training. Therefore, IG training is mandatory for all staff and staff IG training needs should be routinely assessed, monitored and adequately provided for.

Source

- Great Britain (1998) the Data Protection Act 1998 Principle 7 and Schedule I Part II The Stationery Office, London http://www.legislation.gov.uk/ukpga/1998/29/contents

    - Great Britain Department of Health 1997 The Caldicott Report, Review of Patient Identifiable Information Recommendation 2 http://www.google.co.uk/url?url=http://webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/%40dh/%40en/documents/digitalasset/dh_4068404.pdf&rct=j&frm=1&q=&esrc=s&sa=U&ei=xJHkVOCsFpPqaJPwgYgF&ved=0CBQQFjAA&usg=AFQjCNGlrEb5TnxzJPg_5AIzG78tp8Cl-w

- DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information January 2012 https://www.health-ni.gov.uk/publications/code-practice-protecting-confidentiality-service-user-information
- DHSSPS Guidelines for Managing Records in Health and Personal Social Services Organisations in Northern Ireland – Good Management Good Records November 2011 https://www.health-ni.gov.uk/topics/good-management-good-records

GUIDANCE

Information Governance Training

1. IG knowledge and awareness should be at the core of the organisation's objectives, embedded amongst other governance initiatives and should offer a stable foundation for the workforce. Without this knowledge the ability of an organisation to meet legal and policy requirements will be severely impaired.

An Information Governance Training Programme

2. To meet this requirement the organisation should establish a clear plan for IG training appropriately tailored to specific staff groups or job roles. This plan needs to address how and when each work area and/or staff group will be

trained, how training needs beyond the basic level will be assessed and should include induction processes for new staff.

Information Governance Training Needs Analysis

3. Staff inevitably have different levels of awareness of their responsibilities for safeguarding confidentiality, protecting data and preserving information security. Changing established routines and adjusting established work practices can be challenging and it should not be assumed that staff have the knowledge they require. Some staff will require additional training.

4. This needs to be addressed by regular and systematic assessment of training and development needs, consideration of how these needs might best be met and evaluation of any training that has been undertaken.

5. A training needs analysis will generally consist of the following steps:

    a. an assessment of the skills and competencies required to perform a particular job, with emphasis on the importance of that skill-set to the job;

    b. an assessment of the current level of skills and competencies of the staff member performing the job, including relevant professional body memberships or specialist qualifications. For example, online e-learning requires basic IT skills to navigate around a website. If staff are not IT literate then support should be provided to assist;

    c. a comparison of the two assessments and identification of any gaps between the two, i.e. does the person performing the role have, or have access to a person with, sufficient skill and knowledge to enable successful performance;

    d. identification of appropriate training to meet the skills/competency gap.

6. Training needs analyses also allow an organisation to plan regular training programmes in the future where the skills gap identified is a common theme in each area of the organisation.

Staff Induction – Awareness Training

7. Staff induction also needs to address IG training needs as new members of staff may otherwise fail to be picked up by an organisation's rolling training plan. It is vitally important that new staff are made aware of the relevant requirements and in particular given clear guidelines about their own individual responsibilities for compliance. Particular emphasis should be placed on how IG requirements affect their day to day work practices.

8. Induction training should be appropriately tailored for an individual's role both corporately and locally, covering:

a. introduction to IG in every day working environments;

b. the essentials of providing a confidential service to service users in line with the duty of confidentiality;

c. basic information security and records management requirements.

9. And for those staff with routine access to information, training should cover:

a. fundamentals of DP and the Caldicott Principles (see criteria 5);

b. Freedom of Information Act 2000 / The Environmental Information Regulations 2004 responsibilities;

c. principles of good record keeping;

d. information security guidance;

e. pointers to where policies, procedures and further information are located.

Information Governance Training Provision

10. There will inevitably be additional training required, both to help those who need additional support, but also to ensure that staff know how to apply the theory in their own working environments and understand local procedures and where to turn for advice and support.

11. Clearly the ways in which an organisation addresses the provision of training is dependent upon the numbers of staff, their access to confidential information and their assessed training needs. It is important that study time is "protected" so that all employees are able to access and attend appropriate training.

12. Any training that is provided should be regularly reviewed and updated in line with legal requirements, corporate and/or Department of Health (DoH) policy, or any major changes which may impact on the IG agenda, at a local or national level.

13. IG Training should be assessed annually to ensure that appropriate training needs are being met.

Evidence Demonstrating Compliance

For minimal compliance Organisations should evidence that:

- an IG training programme has been developed that includes training needs analyses, induction for new starters and the completion of training on at least one occasion.

In order to move to moderate and then substantive compliance Organisations would be required to evidence that:

- all new staff members have completed IG training. Staff who have undertaken this training on a previous occasion must continue to receive training every three years but this may be locally provided. Training needs are regularly reviewed and re-evaluated when necessary. Training materials and plans must be checked for equivalence to best practice.

- action is taken to test and follow up staff understanding of IG and additional support is provided where needs are identified.

Examples of evidence include:

- named individuals' job descriptions;
- documented training programme;
- training records
- report for senior management;
- minutes of meetings.

These are only examples and it is the responsibility of each organisation to determine how they evidence compliance.

Links with other standards

Governance

ICT Management

Risk Management

Department of Health Information Governance Toolkit Reference - 13-112

Criterion 7

The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs

INFORMATION

Criterion Description

Confidentiality and DP is a key element of the IG agenda. The confidentiality and data protection framework should be supported by adequate skills, knowledge and experience across the whole organisation. The levels of competency should be in line with the duties and responsibilities of particular posts or staff groups to provide an adequate level of assurance.

Source

- Great Britain Department of Health 1997 The Caldicott Report, Review of Patient Identifiable Information Recommendation 2 http://www.google.co.uk/url?url=http://webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/%40dh/%40en/documents/digitalasset/dh_4068404.pdf&rct=j&frm=1&q=&esrc=s&sa=U&ei=xJHkVOCsFpPqaJPwgYgF&ved=0CBQQFjAA&usg=AFQjCNGlrEb5TnxzJPg_5AIzG78tp8Cl-w

- Great Britain Department of Health Health service circular 1999/012 Caldicott Guardians http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Publicationsandstatistics/Lettersandcirculars/Healthservicecirculars/DH_4004311Great Britain (1998) the Data Protection Act 1998 Principle 7 The Stationery Office, London http://www.legislation.gov.uk/ukpga/1998/29/contents

- DHSSPS Letter from Information Management Branch to Chief Executives dated 24/08/09 – Appointment of Personal Data Guardian

- Great Britain Department of Health Health service circular 2000/009 Data Protection Act 1998: protection and use of patient information http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Publicationsandstatistics/Lettersandcirculars/Healthservicecirculars/DH_4002964

- DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information January 2012 https://www.health-ni.gov.uk/publications/code-practice-protecting-confidentiality-service-user-information
- Great Britain Department of Health The Caldicott Guardian Manual 2010 http://systems.hscic.gov.uk/infogov/links/2010cgmanual.pdf

- Information Commissioner Data Protection Audit Manual https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ICO_Data%20Protection%20Audit%20Manual.pdf

- International Standard Organisation International Standard ISO 15489 1:2001(E) Information and Documentation – Records Management http://www.iso.org/iso/catalogue_detail?csnumber=31908

GUIDANCE

Confidentiality and Data Protection Assurance

1. There must be adequate assurance arrangements in place to ensure the most senior level of management in the organisation complies with its current confidentiality and DP obligations and is kept informed of changes and performance which need to be considered and addressed.

Data Protection Act 1998 - Organisational Responsibilities

2. The senior level of management in the organisation, e.g. the Chief Executive, has the ultimate responsibility for compliance with the Data Protection Act 1998 and should ensure that:

    - responsibility for bringing DP issues for consideration by the senior level of management is delegated appropriately, e.g. to a Director or equivalent;

    - a data protection lead or manager is in place to organise and enforce the approach to data protection and report directly to the above individual;

    - the role of Personal Data Guardian is appropriately assigned and supported (see **paragraph 10**).

3. The DP lead/manager has responsibility for ensuring:

    - the successful implementation of the data protection function;

    - a senior person in each unit/department is nominated and responsible for data protection practice within their work area.

4. The unit/department manager is responsible for data protection practice within their work area ensuring:

    - the working practices carried out within the unit/department are in line with the organisation's policy;

    - all staff within the work area are adequately trained and aware of their personal responsibilities for DP issues.

5. It is important that an appropriate individual takes responsibility for directing and pulling together the work necessary to ensure full compliance with the Data Protection Act 1998.

Level of Skills, Knowledge and Experience in Confidentiality and Data Protection

6. The organisation should assess its confidentiality and DP obligations and associated risks to determine the resources needed to establish and maintain the level of assurance required.

7. All staff, including managers, should be made aware of their individual and, if appropriate, managerial accountability for ensuring that confidential personal information (relating to service users or staff) is used in accordance with the relevant organisational policies and procedures.

8. Some staff may require higher levels of awareness, specific training or a professional or other recognised qualification to enable them to carry out their duties to the level required by the organisation e.g. the necessary skills, knowledge and experience to develop corporate strategies, policies or procedures to guide staff. In organisations which face a high volume of complex issues, specialist manager(s), consultant(s) or legal advice may be required. Where such situations are infrequent, this expertise may be better sought 'as and when' required e.g. from a medical defence union or retained legal adviser.

Personal Data Guardians and their Function

9. A key recommendations of the Caldicott Committee (1997 Caldicott Report) was the appointment in each NHS Trust and special health authority of a "Guardian" of patient identifiable information to oversee the arrangements for the use and sharing of patient information and were introduced into social care in 2002. The Personal Data Guardians now in place in HSC bodies have a broadly similar role to perform ensuring the establishment of procedures governing access to, and the use of, identifiable service users' personal information held by the organisation and, where appropriate, the transfer of that information to other bodies set out in a letter to Chief Executives from Information Management Branch dated 24/08/09 – Appointment of Personal Data Guardian.

10. The Guardian should be, in order of priority:

    - a senior health or social care professional;
    - an existing member of the management board of the organisation.

11. It is particularly important that the Personal Data Guardian has the seniority and authority to exercise the necessary influence on policy and strategic planning and carry the confidence of their colleagues.

12. The Guardian plays a key role in ensuring that HSC organisations satisfy the highest practical standards for handling patient identifiable information. Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information.

13. The Personal Data Guardian also has a strategic role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisation's overall governance framework. This role is particularly important in relation to the implementation of national systems and the development of Electronic Care Record and single assessment Frameworks (e.g. NISAT, UNOCINI).

14. In all but the smallest organisations the Personal Data Guardian should work as part of a broader function (see **paragraph 17**) with support staff, or IG leads etc. contributing to the work as required.

15. A Caldicott Guardian manual has been developed by the Department of Health to support their Caldicott Guardians and the Caldicott Function and is applicable to Personal Data Guardians who have a similar role to perform. The Code of Practice on Protecting the Confidentiality of Service User Information (issued in January 2012) provides support and guidance for all those involved in HSC Organisations.

16. The Privacy Advisory Committee (PAC) maintains a register of all the Personal Data Guardians within the HSC. Organisations should ensure the PAC is notified of any changes to their Personal Data Guardian.

Personal Data Guardian Function - Key Responsibilities

-

Strategy & Governance: the Personal Data Guardian should champion confidentiality issues at Board level, should sit on an organisation's Information Governance Board/Group and act as both the 'conscience' of the organisation and as an enabler for appropriate information sharing.
Confidentiality & Data Protection expertise: the Personal Data Guardian should develop a knowledge of confidentiality and data protection matters, drawing upon support staff working within an organisation's Information Governance function but also on external sources of advice and guidance where available.
Internal Information Processing: the Personal Data Guardian should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.
Information Sharing: the Personal Data Guardian should oversee all arrangements, protocols and procedures where confidential personal information may be shared with external bodies both within and outside HSC. This includes flows of information to and from partner agencies, sharing through ICT systems, disclosure to research

interests and disclosure to the police.

Data Protection Key Actions

17. The key actions of the DP work are to:

- ensure compliance with all aspects of the Data Protection Act (DPA) and related provisions and provide reports to the senior level of management in the organisation;
- draft and/or maintain a DP Policy;
- promote data protection awareness throughout the organisation by organising training and providing written procedures that are widely disseminated and available to all staff;
- co-ordinate the work of other staff with data protection responsibilities;
- ensure service users are provided with information on their rights under data protection legislation;
- monitor compliance with the DPA and the effectiveness of procedures through the use of compliance checks / audits and ensure appropriate action is taken where non-compliance is identified;
- lead investigations into complaints about breaches of the DPA;
- ensure notification of information breaches are communicated to the ICO as appropriate.

Data Protection Support Staff

18. Data protection for a large organisation is a major responsibility and the DP Lead requires a degree of support from other staff. These staff members should:

a. carry out the aspects of the work programme delegated to them;

b. attend training as identified through training analyses to keep their skills and knowledge up to date.

Evidence Demonstrating Compliance

For minimal compliance Organisations should evidence that:

- an appropriate Personal Data Guardian has been appointed and there is a documented plan in place for a Personal Data function, which has been approved by senior management or committee.

In order to move to moderate and then substantive compliance Organisations would be required to evidence that:

- the Personal Data Guardian function has adequate confidentiality and data protection skills, knowledge and experience to successfully co-ordinate and implement the confidentiality and DP work programme.

- the confidentiality and DP work programme is incorporated into the broader IG arrangements.

Examples of evidence include:

- named individuals' job descriptions;
- training attendance lists;
- training materials;
- qualification certificates;
- policies and procedures
- strategies;
- report for senior management;
- an IG work plan;
- minutes of meetings.

These are only examples and it is the responsibility of each organisation to determine how they evidence compliance.

Links with other standards

Governance

Department of Health Information Governance Toolkit Reference - 1-200

Criterion 8

The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience

INFORMATION

Criterion Description

Information quality and records management are key elements of the IG agenda. The information quality and records management assurance framework should be supported by adequate skills, knowledge and experience around health/care and corporate records, across the whole organisation. The levels of competency should be commensurate with the duties and responsibilities of particular posts or staff groups to provide an adequate level of assurance.

Source

- Great Britain (1998) the Data Protection Act 1998 Principles 3, 4, 5, and 6 The Stationery Office, London http://www.legislation.gov.uk/ukpga/1998/29/contents

- DHSSPS Guidelines for Managing Records in Health and Personal Social Services Organisations in Northern Ireland – Good Management Good Records November 2011 https://www.health-ni.gov.uk/topics/good-management-good-records
- DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information January 2012 https://www.health-ni.gov.uk/publications/code-practice-protecting-confidentiality-service-user-information
- Cabinet Office – (May 2010) HMG Information Assurance Maturity Model and Assessment Framework https://www.cesg.gov.uk/articles/hmg-ia-maturity-model-iamm
- Public Record Office Northern Ireland (PRONI) – Northern Ireland Records Management Standard https://www.nidirect.gov.uk/articles/records-management-public-bodiesThe National Archives – Standards and Best Practice for Records Managers http://www.nationalarchives.gov.uk/information-management/projects-and-work/standards-records-managers.htm

- DHSSPS The Quality Standards for Health and Social Care Supporting Good Governance and Best Practice in the HSC, March 2006

- General Medical Council, Guidance for Doctors Confidentiality October 2009 http://www.gmc-uk.org/guidance/news_consultation/25893.asp

- Nursing and Midwifery Council The Code, Standards of Conduct performance and ethics for nurses and midwives May 2008 http://www.nmc-uk.org/Nurses-and-midwives/Standards-and-guidance1/The-code/The-code-in-full/
- UK Council for Health Informatics Professionals Code of Conduct http://www.ukchip.org/?q=page/UKCHIP-Code-Conduct

- Information and Records Management Society Information Guides, Resources and consultations http://www.irms.org.uk/resources/information-guides

- International Standard Organisation International Standard ISO 15489 1:2001(E) Information and Documentation – Records Management http://www.iso.org/iso/catalogue_detail?csnumber=31908

GUIDANCE

Information Quality and Records Management – Health/Care Records

1. There must be adequate assurance arrangements in place to ensure the most senior level of management in the organisation complies with its current information quality and records management obligations and is kept informed of changes and performance which need to be considered and addressed.

Information Quality and Records Management Expertise

2. Responsibilities for information quality and records management (clinical, corporate and social services) should be allocated 'appropriately' throughout the organisation. The most 'appropriate' way to achieve this may differ depending on the size and make-up of the organisation and may need to recognise, in some cases, that individuals will be called upon to perform more than one role.

3. Organisations which manage responsibilities for information quality and records management in a different manner may need to be able to justify this and demonstrate that mechanisms are robust.

4. There should be documented strategies in place, with senior management sign-off, to support the information quality and records management work programme which:

    - identifies key individuals and the reporting structure across the organisation to lead on information quality and records management;
    - outlines key aspects of the work programme;
    - identifies the support needed to ensure the work is completed;
    - forms part of the broader information lifecycle policy.

5. This should be supported by an improvement plan which clearly identifies work/actions, responsible individuals and timescales for completion.

Responsibilities for Information Quality Assurance

6. Organisations should ensure that there are individuals with clear responsibility for the quality of service user, staff and corporate data across all systems. There should be a lead strategic focus for information quality assurance through senior management, with a key individual empowered to make operational decisions at director (or equivalent) level.

7. Each person with such responsibility, including those nominated to lead on information quality within new system implementations, must be clear about their roles and their accountability. To this end, job descriptions associated with this role should clearly define accountability and responsibilities for data quality, including monitoring and correction of errors.

8. Individuals with responsibility for information quality should be sufficiently empowered to influence decisions affecting IT systems or information management processes. They should also closely liaise with the organisation's Risk Manager, Education, Training & Development Managers and Department Heads to identify regular or consistent errors by individuals or staff groups, so that retraining needs can be identified and provided for as necessary.

Responsibilities for Records Management

9. There should be individuals with clear responsibility for the management of records within the organisation which includes a lead strategic focus for health or care records, staff and corporate records through senior management, with a key individual empowered to make operational decisions at director (or equivalent) level.

10. Organisations should have Records Managers responsible for:

- identifying current arrangements for managing health/care records or corporate records, including a survey of existing records management systems;
- drafting an organisational records management policy and strategy, which covers all record types;
- liaising and work with other employees responsible for information handling activities, e.g. data protection and the Personal Data Guardian function;
- raising and promoting records management awareness throughout the organisation through profile raising, publicity and by providing training and written procedures that are widely disseminated and available to all staff;
- assessing the need for support staff (e.g. ward clerks, medical secretaries, administrative, clerical, secretarial staff) and their training requirements;

- submitting quarterly performance reports on all record services to the Board.

11. Organisations should:

- facilitate continuity of care by the effective and efficient transmission of information between clinicians/care professionals using the health/care record regardless of the media on which it is held;

- monitoring the health/care records service to ensure that the overall objectives of the organisation and the wider health/care community are met and that the organisation complies with professional good practice, current legislation, national policies and guidelines for good record keeping and management.

- ensure secure management and transfer of corporate records which may contain person identifiable or confidential information;

- monitor working practices to verify accuracy, accessibility, integrity and validity of corporate records. Where there is a lack of compliance with corporate policies, procedures and general best practice guidelines, reviews and assessments should take place to determine how standards should be raised; develop policies and procedures relating to the health/care records and corporate records services, regularly reviewing those policies and amending them as appropriate;

- ensure that all staff are aware of the policies and procedures and that appropriate training is provided;

- develop, implement and regularly monitor standards for the health/care records and corporate services;

- ensure that compliance with the standards is reported regularly to the Senior Management Board (or equivalent);

- ensure that health/care record and corporate record audits are implemented on a regular, systematic basis.

Confidentiality and Data Protection

12. In HSC organisations Records Manager(s) must liaise with the Personal Data Guardian to ensure that the records management strategy and implementation programme is in line with current guidance and protocols on confidentiality.

13. The Records Manager(s) must also work closely with the DP function to ensure that subject access arrangements comply with the Data Protection Act 1998.

Awareness and Training

14. The organisation should assess (and annually review) its legal obligations and associated risks to determine the resources, awareness and training needed to establish and maintain the level of assurance required for managing records and dealing with any requests.

15. Some staff may require higher levels of awareness such as specific training or a professional or other recognised qualification to enable them to carry out their duties to the level required by the organisation. For example, to ensure they have the necessary skills, knowledge and experience to develop corporate strategies, policies or procedures to guide staff or skills required to input clinical information within health/care records. Appropriate training should be provided according to staff job roles, level of access to person identifiable information and responsibilities for processing/managing records.

16. In organisations which face a high volume of complex issues, specialist manager(s), consultant(s) or legal advice may be required. Where such situations are infrequent, this expertise may be better sought 'as and when' required.

17. The HSC Leadership Centre has developed a **Regional eLearning** suite of programmes for IG. The suite of programmes includes Freedom of Information, Data Protection, ICT Security (IT), Records Management (RM) and will be available regionally to those organisations that make up the Information Governance Advisory Group chaired by the DHSSPS Information Management Branch.

18. As well as the interactive e-learning the tool has several other features, including:

    - **Certificate** - on successful completion of each module.
    - **Resource Library** - further reading documents and links to useful websites in relation to FOI.
    - **Reporting function** - for organisation administrators.

    The Tool is available on your organisation's e-learning site.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- appropriately skilled Information Quality and Records Managers/Officers in place and there are documented information quality and records management strategies approved by senior management/committee, which form part of the broader Information Lifecycle Policy.

In order to move to moderate and then substantive compliance Organisations would be required to evidence that:

- there is an appropriate Information Quality and Records Management framework in place with adequate skills, knowledge and experience to successfully co-ordinate and implement the information quality and records management agenda.

- Information Quality and Records Management arrangements are coordinated by the lead manager/officers but are incorporated within broader IG arrangements.

Examples of evidence include:

- named individuals' job descriptions;
- documented policies and strategies
- qualification certificates
- training attendance records
- report for senior management;
- minutes of meetings.

These are only examples and it is the responsibility of each organisation to determine how they evidence compliance.

Links with other standards

Governance

ICT Management

Risk Management

Department of Health Information Governance Toolkit Reference - 13-400

Criterion 9

Contractual arrangements that include compliance with IG requirements are in place with all contractors, support organisations and individuals carrying out work on behalf of the organisation

INFORMATION

Criterion Description

Organisations are responsible for obtaining appropriate contractual assurance in respect of compliance with IG requirements from all bodies that have access to the organisation's information, particularly information about identifiable individuals, or conduct any form of information processing on its behalf. Organisations need to ensure that those undertaking work on behalf of the organisation do so in a lawful manner and meet all appropriate IG requirements. Contracts of permanent, temporary, agency and locum staff should contain clauses that clearly identify responsibilities for confidentiality, data protection and information security. Organisations must ensure that appropriate checks are completed and provide IG training, or request appropriate training is undertaken before permitting them to access systems and information.

Source

- Great Britain (1998) *the Data Protection Act 1998* The Stationery Office, London http://www.legislation.gov.uk/ukpga/1998/29/contents

- DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information January 2012 https://www.health-ni.gov.uk/publications/code-practice-protecting-confidentiality-service-user-information

- ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management 8.1.3 Terms and Conditions of employment contracts http://www.iso27001security.com/html/27002.html

- Great Britain Department of Health 1997 The Caldicott Report, Review of Patient Identifiable Information Recommendation 2 http://www.google.co.uk/url?url=http://webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/%40dh/%40en/documents/digitalasset/dh_4068404.pdf&rct=j&frm=1&q=&esrc=s&sa=U&ei=xJHkVOCsFpPqaJPwgYgF&ved=0CBQQFjAA&usg=AFQjCNGlrEb5TnxzJPg_5AIzG78tp8Cl-w

GUIDANCE

Information Governance Contractual Clauses and Arrangements

1. All organisations need to ensure that work conducted by others on their behalf meet all the required IG standards. Where this work involves access to information about identifiable individuals it is likely that organisations will be in breach of the law where appropriate requirements have not been specified in contracts and steps taken to ensure compliance with those requirements.

2. Organisations must comply with all aspects of the law that are concerned with the processing of personal data. This includes legislation (Acts of Parliament), regulations and common law duties.

Addressing Security in Third Party Agreements

3. Most organisations will, in the course of their business, contract or make arrangements with third parties. The SIRO and IAO should ensure that IG requirements and procedures in outsourcing contracts meet the business needs of the organisation.

4. It is essential that those who work for these third parties are aware of IG requirements; what they can and can't do and who they should contact if things go wrong. Organisation's need to assure themselves that requirements are being satisfied and that contracts and agreements clearly specify what is expected.

5. A risk assessment should be carried out prior to any proposed agreement with a third party. Attention should also be paid if the third party proposes using sub-contractors to provide services in order to undertake the contract. In such cases, the risk assessment must also include those sub-contractors.

6. The SIRO and IAO must take all reasonable steps to ensure that contractors and support organisations to whom personal information is disclosed comply with their contractual obligations to keep personal information secure and confidential. Data protection legislation imposes formal obligations on data controllers that use third party data processors to ensure that the processing by the data processor is carried out under a contract, which is made or evidenced in writing, under which the data processor is to act only on instructions from the data controller.

7. In addition to the contractual performance requirements outlined above, organisations must also ensure that the third party is aware of the possible impact of the Freedom of Information Act 2000 on the documentation connected with that contract.

Key Components of Contracts

8. Contracts should make specific reference to data protection and security issues, such as:

- notification;
- limitations on disclosure and use of data;
- obligations to comply with limits set by the organisation;
- the security and data protection standards that apply to both parties;
- the restrictions placed upon the data processor to act only on instructions from the organisation (the data controller).

Specific reference should also be made within contractual arrangements to freedom of information issues, such as:

- duty to disclose;
- exemption from disclosure provisions;
- records management structure;
- responsibility for FOI applications.

Additionally:

- penalties for breach of the contract;
- a provision to indemnify the organisation against breaches by the third party;
- responsibilities for costs, e.g. for security audit, subject access, for handling information requests;
- specific reference to other relevant legal obligations, e.g. common law duty of confidence, Computer Misuse Act 1990.

Incident Reporting Mechanisms

9. Incident reporting requirements should be included in any contract.

Monitoring and Review of Third Party Services

10. There should be a mechanism in place that provides the organisation with assurances that IG requirements have been met.

11. Monitoring and reviews are designed to ensure that the services in question are being delivered, that controls are being adhered to and to resolve problems or unforeseen events. IAOs should ensure that monitoring is achieved on a regular basis and that good communication is maintained with the third party to ensure issues are resolved efficiently.

Managing Changes to Third Party Services

12. Changes should only take place following authorisation by the nominated IAO, or other accountable personnel within the organisation.

13. Written procedures should detail actions, agreements and authorisation for all changes, whether major or minor.

Information Governance Clauses within Employment Contracts

14. All staff need to be aware that they must meet IG requirements and it should be made clear to them that breaching these requirements, e.g. service user confidentiality, is a serious disciplinary offence.

15. This can be best supported by the inclusion of clauses within staff contracts that cover IG standards and responsibilities with regard to data protection, confidentiality, and information security.

Roles and Responsibilities

16. Health and social care professionals must meet the codes of practice of their professional bodies, and each individual (employees, contractors, locums, etc.) has a personal responsibility to comply not only with the law but also with provisions laid down in their contracts of employment supported by organisational guidelines and documented best practice.

17. If a contract does not explicitly and unambiguously state staff responsibilities, an organisation may have difficulties instigating disciplinary action in the event of an accidental or intentional breach by a member of staff or, in the case of third parties (e.g. staff employed through agencies) who are not directly employed, liabilities due to negligence or misuse. Whilst clearly identifying the responsibilities will not automatically absolve an organisation of all blame, it will be of assistance should an individual deliberately or recklessly breach the law. Therefore, all IG responsibilities for those undertaking work on behalf of the organisation should be defined and documented in contracts.

Screening

18. Screening criteria should be established for jobs, contracts and appointments to ensure that candidates conform to legislation and special requirements (such as security clearances for some positions). The Human Resources/Personnel department is normally responsible for defining the criteria and ensuring that the appropriate checks are carried out. Written procedures should be established to detail these responsibilities. Typically, checks are carried out to verify references, qualifications, identity, criminal record and employment record.

19. If an agency is responsible for checks, the organisation where the individual is working should ensure the appropriate checks are carried out and are subject to regular review. In all cases, prospective employees should be informed in advance of any checks required for a position.

Terms and Conditions of Employment

20. Employment terms should address the following criteria:

a. legal responsibilities, including confidentiality and non-disclosure clauses;

b. information security responsibilities, including encryption, home working and remote access; (where applicable);

c. records management and information quality responsibilities;

d. actions to be taken if the employee, contractor or third party user disregards the organisation's IG standards.

Management Responsibilities

21. Individuals must be made aware of their responsibilities through documentation, training and awareness sessions, including induction, and other awareness materials (see **criteria 6**). In the case of dealing with sensitive information, wherever practicable the organisation should ensure that training is provided before access is granted. Training, education and awareness materials should be regularly updated.

Disciplinary Process

22. A formal disciplinary process should be in place and documented procedures made available to all staff. IG breaches should be clearly referenced and staff left in no doubt about the consequences of misconduct.

Termination or Change of Employment Responsibilities

23. There should be written procedures for managing changes to, or termination of staff employment. They should include procedures for the return of all assets (equipment, documentation, smartcards, office keys, etc) which were issued to employees and recorded in the data asset register and access rights required until the last day of employment.

24. Should an employee or contractor's employment be terminated, management should take actions to ensure information and facilities are not misused, corrupted or destroyed.

Evidence Demonstrating Compliance

For minimal compliance Organisations should evidence that:

- All contractors or support organisations (including non-clinical staff) with access to the organisation's information assets have been identified and appropriate clauses for inclusion in contracts have been developed. All current and new employment contracts contain appropriate IG compliance requirements, and there is a plan to ensure that individuals working on behalf of the organisation understand their responsibilities

In order to move to moderate and then substantive compliance Organisations would be required to evidence that.

- Appropriate clauses on compliance with IG have been put into all contracts and/or agreements. The action plan has been implemented and all existing staff are aware of their obligations for IG. Appropriate checks are completed on all new staff, they are appropriately, trained and provided with guidelines to ensure they are aware of their obligations for IG before they start handling person identifiable information.

- Reviews and/or audits are conducted to obtain assurance that all third parties that have access to the organisation's information assets are complying with contractual IG requirements. Staff awareness of their responsibilities and their compliance with IG requirements is checked and monitored.

Links With Other Standards

Risk Management

Department of Health Information Governance Toolkit Reference - 13-110

Criterion 10

As part of the information lifecycle management strategy, an audit of corporate records has been undertaken

INFORMATION

Criterion Description

Good records management practice necessitates that organisations should undertake an audit of records management processes and systems. This determines what records are held, where they are located and in what form they are held. The audit will assist in compliance with legal provisions, such as the Freedom of Information Act (FOIA) 2000.

Source

- DHSSPS Guidelines for Managing Records in Health and Personal Social Services Organisations in Northern Ireland – Good Management Good Records November 2011 https://www.health-ni.gov.uk/topics/good-management-good-records
- Public Record Office Northern Ireland Guidelines on Information Audits and Disposal Schedules for Northern Ireland Public Authorities 2003 https://www.nidirect.gov.uk/publications/guidelines-information-audits-and-disposal-schedules-northern-ireland-publicPublic Record Office Northern Ireland (PRONI) – Northern Ireland Records Management Standard https://www.nidirect.gov.uk/articles/records-management-public-bodiesThe National Archives – Standards and Best Practice for Records Managers http://www.nationalarchives.gov.uk/information-management/projects-and-work/standards-records-managers.htm

- The National Archives – Complying with the Records Management Code Evaluation Toolkit February 2006 http://www.nationalarchives.gov.uk/documents/full_workbook.pdf

- International Standard Organisation International Standard ISO 15489 1:2001(E) Information and Documentation – Records Management http://www.iso.org/iso/catalogue_detail?csnumber=31908

- Great Britain (2000) The Freedom of Information (FOI) Act 2000 The Stationery Office, London http://www.legislation.gov.uk/ukpga/2000/36/contents

- Great Britain (2004) Environmental Information Regulations 2004 The Stationery Office, London http://www.legislation.gov.uk/uksi/2004/3391/contents/made

- Great Britain. Lord Chancellors Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000. (2009) London: The Lord Chancellor's Department.