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.

http://www.nationalarchives.gov.uk/information-management/projects-and-work/records-management-code.htm

GUIDANCE

Auditing Corporate Records

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

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

Purpose of the Records and Information Audit

2. Organisations should carry out an audit of corporate records and information, to establish:

    - the type of records currently held;
    - the form in which they are held;
    - the record keeping systems currently in use, how effective they are and those that need to be developed/updated/procured.

3. Organisations should ensure that current corporate records and closed/archived records are surveyed. The audit should include paper and electronic records collections, for example, records in filing cabinets, storage rooms, databases, web sites and shared network filing areas.

4. A records audit should enable the organisation to:

    - ensure corporate record retention periods are in line with Good Management Good Records;

- identify the location of records to assist the organisation to respond promptly to Freedom of Information requests;
- determine the use made of each category of corporate record;
- determine whether duplicate records exist;
- determine whether it is necessary to retain the record;
- assess current and future records storage requirements;
- identify record creation and disposal concerns;
- identify the department responsible for creation, use and management of each record collection;
- create an information asset register;
- identify any information security concerns.

5. Another objective of the records audit is to ensure that the organisation has complete and accurate corporate records to:

- enable internal and external audit;
- protect the legal rights of the organisation, its employees, its service users and third parties;
- provide authentication so that actions may confidently be taken on reliable information.

6. Actions taken to deal with identified problems should feed into the organisation's information lifecycle management strategy (see **Governance**).

7. The records audit may reveal information held by or on behalf of another organisation, which may assist when responding to Freedom of Information requests (see **criteria 4**).

A Records Audit

8. The best approach to an audit of corporate records and information may be to set it up as a work programme in its own right. However, first there must be a formal commitment from senior managers supporting the process and delegating responsibility for coordinating and carrying it out to an appropriate member of staff.

9. To ensure the audit works effectively and achieves its aims, organisations should consider using established project management methodology and as such a Project Initiation Document (PID) and project plan should be developed and signed off by senior management. The PID and project plan

should outline the commitment to allocate the necessary resources, both financial and human, to carry out the work and will need to identify:

- the aims and objectives of the audit;
- how staff members in relevant areas will be informed of the audit;
- the staff members/job roles responsible for undertaking the audit;
- how the audit will be carried out, for example, visits, questionnaires, interviews;
- the order that departments will be surveyed, (e.g. are there particular corporate areas that need to be done first?);
- the timescales for completion;
- how the finished work will be presented;
- who the finished audit will be presented to.

10. Once the PID and project plan have been signed off by senior managers and staff members in relevant areas have been effectively informed, work should commence based on the PID and project plan.

Performing the Audit

11. There are several ways in which an organisation may want to carry out the audit. An initial walk-through visit to the department selected for audit will enable the organisation to:

- see where paper and electronic records are stored;
- assess the general condition of stored paper records;
- obtain an overview of the types of information captured in the record.

12. Questionnaires and/or interviews can be used to gather detailed data, for example:

- who “owns” the record?
- how old is the record, i.e. what are the covering dates?
- is it still in use?
- is it of historical interest?

13. A records audit survey template and forms are available in the Department of Health Information Governance Toolkit. For electronic records see

http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/records/electronicsurvey.xls and for manual records see http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/records/manualsurvey.xls

14. To assess the effectiveness of the audit methodology, organisations may wish to audit one corporate area first as a pilot.

15. It might be necessary to carry out follow-up interviews once the records audit survey results have been returned to the team co-ordinating the work.

16. A representative sample of the categories of record created by the chosen area should be tracked through the various departments and personnel that handle it, with particular emphasis on the type of information, what it is used for and, if it is passed on, who it is transferred to. If the information is copied or stored by any of the departments this should also be recorded, as this will assist organisations to more easily locate duplicates.

17. By tackling the work in “chunks”, an organisation can incrementally begin to build up a picture of corporate records, the information it holds and the information it sends and receives.

18. A report should be presented to the Board, senior management team or delegated sub-group, so that a decision can be made about the allocation of resources necessary to continue the work. The rate at which the organisation can audit further information and records will obviously depend on the resources available.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- there is a project initiation document (PID) and project plan in place, which includes the allocation of resources, for the completion of an organisation-wide corporate records audit.

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

- An audit of corporate records has been undertaken in several (at least four) corporate areas of the organisation (see **paragraph 1** of the guidance to this requirement.

- An audit of all corporate records has been carried out providing a comprehensive understanding of all the corporate records held. A full report has been produced for senior management or Board for review and sign off and an improvement plan has been developed to tackle any identified problem areas that have not already been dealt with.

Examples of evidence include:

- named individuals' job descriptions;
- documented project plan;
- 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

Department of Health Information Governance Toolkit Reference - 13-604

Criterion 11

There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data

INFORMATION

Criterion Description

Under section 7 of the Data Protection Act 1998, subject to certain conditions, an individual is entitled to be informed whether personal data about them is being processed by or on behalf of the data controller. Organisations must have procedures in place to ensure that individual's rights of access are met within a timely and appropriate fashion.

Source

- 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 http://www.legislation.gov.uk/uksi/2000/415/contents/made
- 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 The Quality Standards for Health and Social Care Supporting Good Governance and Best Practice in the HSC, March 2006

GUIDANCE

Introduction

1. If their personal data is being processed, the individual has the right to be given a description of the data, the purposes of the processing and if the information is to be shared, who it will be shared with. The individual is also entitled to apply for access to personal data of which they are the subject.

2. Access encompasses the following rights, to:

    a. obtain a copy of the record in permanent form;

    b. have information provided in an intelligible format (and explained where necessary, e.g. medical abbreviations).

3. Where the individual agrees, the access right may be met by providing a facility for the individual to view the record without obtaining a copy.

Compliance with the Data Protection Act 1998

4. Under the Act the request must be complied with within 40 calendar days of the organisation receiving it, or in any case within 40 calendar days of receipt of any further information required to identify the correct individual.

5. To assist the obligation to provide information within the time limits, organisations must ensure that all employees are aware of how a subject access request should be made and of the requirement to respond to requests quickly.

6. The organisation should determine where subject access requests are more likely to be made and ensure that awareness training is provided to all staff in those areas. Staff in areas where requests are ultimately handled must be provided with comprehensive training. The training should cover:

    a. required format of a subject access request;

    b. correct identification of the requesting individual;

    c. location of personal information;

    d. timescales for compliance;

    e. provision of information in an intelligible format;

    f. action to be taken if the information includes third party data or if it has been determined that access will seriously harm an individual (see exemptions in **paragraph 10**).

7. The organisation should ensure that the subject access procedures are reviewed regularly, and implement additional procedures to assess and improve performance in meeting the statutory timeframes (or any more restricted timeframes required by the subject access request procedures).

Making an Access Request

8. Individuals wishing to exercise their right of access should:

    a. make a written application to the organisation holding the records, including via email;

    b. provide such further information as the organisation may require to sufficiently identify the individual;

    c. pay the relevant fee upon request.

9. The maximum fee that may be charged for providing copies of a record which is held entirely in computerised format is £10. For healthcare records held partially or entirely on paper, the maximum amount that may be charged is £50. For social care records held in any format the maximum fee is £10.

Exemptions

10. Generally, the organisation should provide information to the individual except where an exemption preventing or restricting access applies. Access may be denied or restricted where:

    a. the record contains information which relates to or identifies a third party that is not a care professional and has not consented to the disclosure. If possible the individual should be provided with access to that part of the record which does not contain the third party information.

    b. access to all or part of the record will prejudice the carrying out of social work by reason of the fact that serious harm to the physical or mental well-being of the individual or any other person is likely. If possible the individual should be provided with access to that part of the record that does not pose the risk of serious harm.

    c. access to all or part of the record will seriously harm the physical or mental well-being of the individual or any other person. If possible the individual should be provided with access to that part of the record that does not pose the risk of serious harm.

DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information January 2012

11. Individuals' rights regarding the sharing of their personal information are supported by the DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information January 2012. It provides support and guidance for all those involved in health and social care for protecting and safeguarding service user information, particularly in regard to individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

Complaints and Appeals

12. The organisation should ensure that its procedures set out the individual's right to appeal against a decision to refuse access to their information and the way in which an appeal or a complaint about the subject access procedures should be made.

13. Responsibility for dealing with complaints and appeals should be appropriately assigned within the organisation. For example, initial complaints about data protection procedures and appeals against decisions not to allow

access to information made to the Data Protection Lead. If the Lead is unable to resolve the issue the complaint/appeal should be referred to the IG forum (or equivalent) or if appropriate, to a senior medical or social care professional for consideration.

14. The Information Commissioner's Office is the independent Ombudsman with responsibility for data protection issues, therefore the organisation's complaints and appeals procedure should provide individuals with the following contact details.

Post: Information Commissioner's Office - Northern Ireland
3rd Floor
14 Cromac Place,
Belfast
BT7 2JB

Telephone: 0208 9027 8757 / 0303 123 1114
Email: ni@ico.gsi.gov.uk

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- there is a documented procedure for handling subject access requests 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:

- subject access requests are actioned by fully trained and resourced staff and all staff members are aware of the need to support subject access requests, and where in the organisation such requests should be directed. The procedure has been implemented effectively to meet the statutory deadlines.

- the subject access procedure is regularly reviewed, and where necessary, additional measures have been implemented to assess and improve performance in meeting the statutory timeframes (or any more restricted timeframes required by the subject access request procedure).

Examples of evidence include:

- named individuals' job descriptions;
- documented procedures;
- 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

Department of Health Information Governance Toolkit Reference - 13-205

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.

INFORMATION

Criterion Description

There are legal restrictions on how personal information may be used stemming from the Data Protection Act 1998, and where personal information is held in confidence (e.g. to provide care and treatment), the common law places additional constraints on its disclosure. Usually a form of consent is required, unless the disclosure is required by Court Order or Legislation. Staff must be made aware of the right of an individual to restrict how confidential personal information is disclosed and the processes that they need to follow to ensure this right is respected.

Source

- The common law duty of confidence
- 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
- DHSSPS & HSC Protocol for Sharing Service User Information for Secondary Purposes https://www.dhsspsni.gov.uk/publications/dhssps-hsc-protocol-sharing-service-user-information-secondary-purposesInformation Commissioner's Office Guidance for Health Sector Organisations http://www.ico.org.uk/for_organisations/sector_guides/health
- DHSSPS Reference Guide to Consent for Examination, Treatment or Care March 2003 http://www.dhsspsni.gov.uk/consent-referenceguide.pdf

GUIDANCE

Use and Disclosure of Personal Information

1. The Data Protection Act 1998 provides conditions that must be satisfied prior to using or disclosing, (both termed processing in the Act), personal information. Where personal information is held in confidence (e.g. health records or case file information) common law obligations additionally require

the consent of the subject of the information before it is disclosed to a third party unless exceptional circumstances apply.

Data Protection Act 1998 Conditions

2. The Data Protection Act 1998 provides eight Principles that apply to all use and disclosure of personal information. In addition to satisfying these eight Principles, organisations must also satisfy one condition from a supplementary schedule (schedule 2 of the Act) and where the information is deemed sensitive personal information under the provisions of the Act a further condition from a second supplementary schedule (schedule 3) must be satisfied. It is important to note that where a care organisation is using and disclosing personal information for purposes relating to the care of an individual the Act will not prevent that use or disclosure.

Common Law Obligations

3. The Common Law requires that there is a lawful basis for the disclosure of personal information that is held in confidence. Normally the basis of access will be consent which must be sought before disclosure of the information. It is generally accepted that this consent can be implied where the purpose is directly concerned with an individual's care or with the quality assurance of that care and the disclosure should not reasonably surprise the person concerned. The provision of information – see criteria 13 depending on organisation type – is also important in this context to reinforce the basis for implying consent. Consent **cannot** be implied when an individual has expressly refused to the processing of their personal information.

4. In other circumstances and for other purposes consent cannot be implied and so must be specifically sought or there must be some other lawful basis for disclosing the information.

Using the Information for Purposes Unconnected to Care Services

5. Where an organisation wishes to disclose confidential personal information for a purpose unrelated to care, consent cannot be implied. In most cases, individuals should be asked for their explicit consent for information to be shared with non-care organisations, for example:

    - housing departments;
    - education services;
    - voluntary services;
    - Sure Start teams;
    - the police;
    - government departments.

Examples of Non-care purposes
Checking quality of care • Testing the safety and effectiveness of new treatments and comparing the cost-effectiveness and quality of treatments in use; • Care audit activity on site; • Supporting Regulation and Quality Improvement Authority (RQIA) audit studies; and • Ensuring the needs of service users within special groups are being met e.g. children at risk, chronically sick, frail and elderly.
Protecting the health of the general public • Drug surveillance and other research-based evidence to support the regulatory functions of the Medicines and Healthcare products Regulatory Agency; • Surveillance of disease and exposures to environmental hazards or infections and immediate response to detected threats or events; • Vaccine safety reviews; • Safety monitoring of devices used in healthcare; • Linking with existing National Registries for diseases / conditions; • Analysis of outcomes following certain health interventions (i.e. public health interventions as well as treatments); • Monitoring the incidence of ill health and identifying associated risk factors; and • Identifying groups of service users most at risk of a condition that could benefit from targeted treatment or other intervention.
Managing care services • Capacity and demand planning; • Commissioning; • Data for Standards and Performance Monitoring; • Clinical indicators; • Information to support the work of the RQIA; • Evidence to support the work of the National Institute for Health and Clinical Excellence;

• Measuring and monitoring waiting times; • Data to support Productivity Initiatives; • Personnel Records; • Agenda for Change; and • Benchmarking.
Supporting research • Assessing the feasibility of specific clinical trials designed to test the safety and/or effectiveness and/or cost-effectiveness of healthcare interventions; • Identification of potential participants in specific clinical trials, to seek their consent; • Providing data from routine care for analysis according to epidemiological principles, to identify trends and unusual patterns indicative of more detailed research; • Research Ethics Protocols/procedures and • Providing specific datasets for defined approved research projects.

6. Where explicit consent cannot be obtained the organisation may be able to rely on the public interest justification or defence. This is where the organisation believes that the reasons for disclosure are so important that they override the obligation of confidentiality (e.g. to prevent someone from being seriously harmed). There is more information on public interest disclosures available in the Code of Practice on Protecting the Confidentiality of Service User Information.

7. Disclosure may also be required where there is a statutory or other legal basis for the disclosure.

8. The advice of specialist staff, e.g. Personal Data Guardians or legal advisors should be sought prior to making disclosures in the public interest or where a Court Order or statutory basis is provided as justification.

9. In general no-one may consent on behalf of another individual who has the capacity and competence to decide for themselves. However, treating clinicians, parents of young children, or legal guardians must make decisions that they believe are in the best interests of the person concerned. The Mental Capacity Act 2005 and the Department of Health document 'Reference Guide to Consent for Treatment or Examination' do not apply in NI, but work is under way to bring forward similar legislation for NI, incorporating mental capacity and mental health provisions. The DoH guidance 'Reference Guide to Consent for Examination, Treatment or Care (2003)', which is available on the DoH website, gives advice on determining whether a person has capacity and what action may be taken where the person lacks capacity. Available from: http://www.dhsspsni.gov.uk/consent-referenceguide.pdf

10. It should also be borne in mind that an individual has the right to change their mind about a disclosure decision at any time before the disclosure is made, and can do so afterwards to prevent further disclosures where an activity requires a regular transfer of personal information.

11. The PAC in Northern Ireland can advise on the sharing of information; but it has no statutory powers and so cannot give lawful authority to disclosures of identifiable information without consent. In the event of a complaint or challenge, its advice on best practice might play an important part in any assessment of the appropriateness of a disclosure.

Staff Guidelines on Respecting Disclosure Decisions

12. To ensure individuals' rights to restrict disclosure of their personal information are respected, staff should be made aware of these rights and be provided with guidelines included in the organisation's confidentiality code of conduct or equivalent (see **criteria 5**). The guidelines should address:

    - when and how consent should be obtained;
    - the basic premise that individuals have the right to choose whether or not to agree to the disclosure of their personal information;
    - the right of individuals to change their decision about a disclosure before it is made;
    - who should obtain consent for the further purpose;
    - where and how consent or refusal to consent should be recorded;
    - answering questions about consent including how to provide information about the consequences of non-disclosure in a non-threatening, non-confrontational manner;
    - how often consent should be reviewed;
    - any sanctions for failure to respect individuals' disclosure decisions;
    - other lawful reasons for disclosure of confidential personal information - public interest, or legally required.

Services Provided by Third Parties

13. Where an organisation contracts with a third party to provide care services the contracts must prevent personal information from being used for purposes other than those contracted for and must also ensure that there is explicit consent or some other lawful basis for disclosure where required.

Evidence Demonstrating Compliance

For minimal compliance Organisations should evidence that:

- there are guidelines for staff on when it is both lawful and appropriate to share confidential personal information and on respecting service user wishes. The guidelines have been approved by senior management or an appropriate committee.

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

- the documented and approved guidelines have been made available at appropriate points in the organisation and all staff members have been effectively informed about the need to comply with them.

- staff compliance with the guidelines is monitored to ensure, unless there is a legal reason not to, they respect service user choices when disclosing confidential personal information.

Examples of evidence include:

- named individuals' job descriptions;
- a copy of the guidance;
- codes of practice
- contracts
- 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 - 13-202

Criterion 13

Individuals are informed about the proposed uses of their personal information

INFORMATION

Criterion Description

Organisations should have communication materials that clearly and concisely inform individuals about the way that their information is used and shared, and their rights in terms of access and to prevent disclosure or use.

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

- 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.pdfhttp://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/2010cgmanual.pdf

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

GUIDANCE

Ensuring Individuals are effectively informed

1. Individuals must be informed, in general terms, how their information may be used and the organisations or types of organisation it may be disclosed to. This is required by the Data Protection Act 1998 (termed Fair Processing in the Act) but also to provide a basis for implying consent for using and sharing information for care purposes in order to satisfy common law requirements.

2. The communications between the organisation and its service users about recorded information should therefore be two-way and proactively managed. The approach to achieving and maintaining effective communications should

be outlined within an organisation's overall IG policy and strategy. The term service user needs to be considered in relation to the services your organisation provides.

3. Materials should be displayed prominently in areas where individuals will see them, for example, in waiting areas and receptions. The awareness campaign should be supported by procedures to ensure that if more detailed explanations are required individuals can access the required information or be guided towards a staff member who is able to answer their queries.

4. Organisations should undertake a robust assessment of the needs of people with special/different needs and the communications materials designed to meet them. It may be that the information is required in several formats, for example:

    - different languages;
    - in Braille;
    - on audio tape;
    - in large print.

5. Or it may be necessary for the organisation to have access to a translator, e.g. for those service users who:

    - use sign language;
    - have difficulty conversing in English and are also unable to read in their native language.

Raising Awareness Amongst Staff

6. To ensure individuals are properly informed, staff must themselves be familiar with the content of local communication materials. Therefore, organisations should ensure that all relevant staff members receive guidance on how to:

    - make clear to individuals when information is recorded or accessed;
    - make clear to individuals when information is or may be disclosed to others;
    - check that individuals are aware of the choices available regarding the use of their information;
    - check that individuals have access to the communications materials, e.g. leaflets, posters;
    - deal with concerns or queries, including referral to other staff members;
    - respect the right of individuals to have access to their health records or case files.

Raising Awareness Amongst Service Users

7. The starting point for an awareness raising campaign is the use of general communication materials to inform individuals accessing services about the use of their personal information for care services and of any known circumstances under which information could be used for purposes

unconnected to the provision of care services (see criteria 12). The materials may be in the form of leaflets, posters, inserts with appointment letters or text on appointment cards, etc.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- general communication materials are available to inform individuals accessing services about the use of their personal information.

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

- the general communication materials are supported by an active communications campaign to inform all individuals, including those with special/different needs, about how their personal information is used.

- staff compliance with their responsibilities to ensure individuals have access to the communications materials about the use of personal information is monitored and assured.

Examples of evidence include:

- named individuals' job descriptions;
- a copy of the leaflet, poster, or other written material ;
- communications 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

Department of Health Information Governance Toolkit Reference - 13-203

Criterion 14

Where required, protocols governing the routine sharing of personal information have been agreed with other organisations

INFORMATION

Criterion Description

When confidential personal information that can identify an individual is shared, both the disclosing and receiving organisations should have procedures that meet the requirements of law and guidance and make clear to staff the appropriate working practices. In some circumstances these procedures (and the law and guidance on which they are based) should be set out within an agreed information sharing agreement or protocol. The DHSSPS and HSC Protocol for Sharing Service User Information for Secondary Purposes should be implemented and communicated throughout the organisation and Data Access Agreements developed consistently in line with the protocol.

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

- 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-purposesGreat 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 The Caldicott Guardian Manual 2010 http://systems.hscic.gov.uk/infogov/links/2010cgmanual.pdfhttp://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/2010cgmanual.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

- Ministry of Justice Public Sector Data Sharing: Guidance on the Law http://www.justice.gov.uk/downloads/information-access-rights/data-sharing/annex-h-data-sharing.pdf

- Information Commissioner's Office Anonymisation: Managing Data Protection Risk Code of Practice November 2012 **GUIDANCE**

Introduction

1. There are specific legislative requirements in relation to organisation's obligations under the Data Protection Act 1998. There are 8 principles, the first of which requires that all pers**onal data** is processed "fairly" and "lawfully". Any processing including sharing of service user identifiable information must be lawful and organisations must ensure they have the legal powers to process the information for the purpose intended.

2. Government policy places a strong emphasis on the need to share relevant personal information across organisational and professional boundaries, in order to ensure effective co-ordination and integration of public services. It also emphasises the importance of security and confidentiality in relation to personal information.

Information Sharing Protocols

3. Organisations will need to share confidential person-identifiable information with a range of others for the provision of care, including the quality assurance of that care, for the individual concerned or for non-care or secondary purposes, e.g. service evaluation, research, finance, public health work etc.

4. It is recommended that information sharing protocols are in place when sharing information between organisations in order to ensure that the 'rules' are clearly understood and that the requirements of law and guidance are being met. They provide a transparent and level playing field for organisations that need to exchange information and provide assurance in respect of the standards they adopt.

5. Information sharing protocols generally have three tiers or elements:

    - a high level statement signed by the Personal Data Guardian, which provides assurance that the organisation will comply with the terms of the protocol;

    - a description of the principles and rules that will be followed, consent procedures, legal compliance, security requirements etc;

    - guidance for staff on how to conduct day to day business with partner organisations who are party to the protocol.

6. Individuals' rights regarding the sharing of their personal information must be supported by high-level commitments for protecting and safeguarding service user information, particularly in regard to individuals' rights of access to their

own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

Sharing to Provide Care

7. There are various reasons why information needs to be shared when providing direct care to service users. HSC organisations are not required to have information sharing protocols in place when sharing information for the purposes of direct care, although a protocol can support the day to day operational activity in sharing information.

Sharing for Non-care Purposes

8. In November 2011 the DHSSPS developed a protocol for sharing service user information for secondary purposes in conjunction with representatives from the Non – Departmental Public Bodies. The aim of the protocol is to support and embed the principles and guidelines of the Code of Practice on Protecting the Confidentiality of Service User Information and to assist the DoH, HSC and Public Safety bodies to comply with the Code of Practice. (For the purposes of the protocol the Department, HSC and Public Safety bodies covered by the protocol are known as partner organisations.)
The protocol is a resource that will help support staff when making decisions about information sharing, promote best practice and ensure a consistent approach to information sharing across the HSC sector in NI.

9. The protocol should assist partner organisations in establishing 'on the ground' procedures for sharing data between them and will be activated through Data Access Agreements (DAAs) for specific service areas between organisations. A standard Data Access Agreement template has been developed in line with the requirements of the protocol and is included in the protocol at appendix 2.

10. The Code of Practice on Protecting the Confidentiality of Service User Information contains examples of cases when staff may need to disclose personal information for secondary uses or other purposes. Staff should also follow the flow diagram included at appendix 5 of the protocol which covers the key considerations in making good decisions about the use and disclosure of identifiable service user information.

11. The Protocol requires each partner organisation to have a nominated senior professional, which where possible should be a Personal Data Guardian who is responsible for:

    - approving who in their organisation has access to the shared information;
    - approving amendments to the protocol;
    - ensuring mechanisms are in place to monitor its operation and ensure compliance; and

- reporting to relevant parties on any breaches and action taken.

12. There is a need to ensure that the protocol is implemented fully and communicated throughout the organisation. To provide this assurance there must be internal monitoring to ensure:

    - the protocol is activated through Data Access Agreements and they are consistent with the protocol;
    - the protocol supports the required performance;
    - that all information sharing follows the requirements of the protocol;
    - that the protocol is made available to all staff and service users and that staff are appropriately trained;
    - that internal arrangements support the protocol and ensure that staff adhere to these arrangements; and
    - Where the sharing of information is lawful, ensure through mutual agreement that information sharing is fully supported and facilitated.

13. Organisations should assure themselves that the requirements of the sharing protocol are being adhered to.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- the Personal Data Guardian oversees the implementation of the protocol within the organisation and is responsible for signing off the organisations Data Access Agreements.

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

- Data Access Agreements are up to date and data destruction notifications which form part of the agreement have been received and are up to date.
- the Personal Data Guardian is taking responsibility for actively reviewing the Protocol and Data Access Agreements.

Examples of evidence include:

- Named individuals' job descriptions;
- report for senior management;

- data Access Agreements;
- Data Destruction Notifications
- reports
- 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 - 13-207

Criterion 15

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

INFORMATION

Criterion Description

Organisations are responsible for the security and confidentiality of personal information they process. Processing may include the transfer of that information to countries outside of the UK, and where person identifiable information is transferred, organisations must comply with both the Data Protection Act 1998 and the Department of Health guidelines.

Source

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

- Information Commissioner's Office Data protection guidelines International transfers of personal information: General advice on how to comply with the 8th data protection principle October 2008 https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf
-

GUIDANCE

Transfers outside the UK

1. The Data Protection Act 1998 implements into UK law Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The aim is to harmonise data protection laws so that potential obstacles to cross-frontier flows of personal data between member states of the European Union (EU) are reduced and a high level of data protection within the EU is ensured.

2. Principle 8 of the Act governs transfers of personal information and requires that it is not transferred to countries outside of the European Economic Area unless that country has an adequate level of protection for the information and for the rights of individuals.

The European Economic Area

3. The European Economic Area (EEA) is made up of the EU member states plus the European Free Trade Association (EFTA) countries of Iceland, Liechtenstein and Norway. The current EU member states are in Table 1.

Table 1: The European Union Member States				
Austria	Belgium	Bulgaria	Cyprus	Czech Republic
Denmark	Estonia	Finland	France	Germany
Greece	Hungary	Ireland	Italy	Latvia
Lithuania	Luxembourg	Malta	Netherlands	Poland
Portugal	Romania	Slovakia	Slovenia	Spain
Sweden	United Kingdom			

4. Further details can be found on the EEA website.

An Adequate Level of Protection

5. The European Commission has the power to determine whether a third country (i.e. not an EU member state or an EFTA country) ensures an adequate level of protection for personal data by reason of its domestic law or the international commitments it has entered into.

6. The Commission has so far recognised Switzerland, Canada, Argentina, Guernsey, Isle of Man, Jersey, the US Department of Commerce's 'Safe Harbor' Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection.

7. Information on countries with an adequate level of protection and the US Safe Harbor agreements can be found within the European Commission decisions on the adequacy of the protection of personal data in third countries.

8. To ensure compliance, where an organisation discovers that it does transfer personal data to a country not listed in **Table 1** above, it should check the website referred to in **paragraph 7** to obtain up to date information about whether the country is deemed to have adequate protection.

9. If the transfer is to a third country not on the adequacy list, the organisation should put measures in place to ensure that there is an adequate level of protection when person identifiable information is transferred. This requires that contractual agreements are drawn up specifying the terms on which the information is transferred and the restrictions on its use for further purposes.

10. The organisation should assess all risks to the information and put protective measures in place to reduce any risks. Potential risk areas to be taken into account include:

    a. what information is being transferred?

    b. have the data subjects been informed?

    c. to what country is the information being transferred?

    d. what are the purposes of the transfer?

    e. what data protection laws are in place in the overseas country?

    f. is data protection appropriately covered in the contractual arrangements between the organisations?

    g. is restriction on further use appropriately covered in the contractual arrangements between the organisations?

    h. how is the information to be transferred?

    i. what security measures are in place to protect the information during transfer?

    j. what security measures are in place in the recipient organisation?

11. Further guidance is available from the Information Commissioner's Office detailed specialist guide, 'The Eighth Data Protection Principle and International Data Transfers'.

Department of Health Guidelines

12. The DoH endorses the following guidelines issued by the Department of Health (DoH) and requires organisations to comply with them.

    a. Person identifiable information must not be transferred outside of the UK unless appropriate assessment of risk has been undertaken (see **paragraph 10**) and mitigating controls put in place.

    b. The organisation should review the flows of person identifiable information identified for **criteria 16**, dependent on organisation-type, to understand whether information transferred to external organisations flows outside of the UK.

    c. Information about overseas transfers of information must be included within the organisation's Data Protection notification to the Information Commissioner and should ideally be included within the organisation's IG Policy or equivalent document.

d. Decisions on whether to transfer person identifiable information must only be taken by a senior manager or senior care professional that has been authorised to take that decision.

e. Organisations will need to obtain an assurance statement from third parties that process the personal data of their service users or staff overseas. This assurance may be within the contract between the two organisations or within other terms of processing.

Data Protection Act Principles

13. Whilst compliance with the eighth Principle is crucial, organisations must also consider all the other Data Protection Principles before making an overseas transfer of person identifiable data.

14. Of particular importance is the first Principle, which in most cases will require that individuals are properly informed about the transfer of their information to a country outside the UK.

Determining whether measurement of the criteria is required

15. Organisations acting purely as a data processor on behalf of a data controller should only be processing personal data in accordance with their contractual agreement with the data controller. Therefore, it is the data controller who is responsible for assessing their organisation against this requirement. Data processors must still comply with the other Data Protection principles.

16. Those organisations which act as data controllers, joint data controllers or data controllers in common must assess themselves against this requirement and ensure any overseas transfers of information are notified to the Information Commissioner.

17. Where an organisation has determined that it makes no transfers of personal information to non-UK countries this should be documented for audit purposes, provided as evidence and the controls assurance returned marked not appropriate as measurement against this criteria will not be required.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- all transfers of personal information to countries outside the UK have been documented, reviewed and tested to determine compliance with the Data Protection Act 1998 and the Department of Health (DH) guidelines in paragraph 12.

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

- all transfers of personal data to countries outside of the UK fully comply with the Data Protection Act 1998 and DH guidelines in paragraph 12. Where the review of overseas transfers reveals that appropriate contracts are not already in place for existing transfers, the organisation ensures that new contractual arrangements are signed.

- transfers of personal data to non-UK countries are regularly reviewed to ensure they continue to fully comply with the Data Protection Act 1998.

Examples of evidence include:

- named individuals' job descriptions;
- 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

Department of Health Information Governance Toolkit Reference - 13-209

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

INFORMATION

Criterion Description

To adequately protect transfers / flows of information, organisations need to identify the transfers, risk assess the transfer methods and consider the sensitivity of the information being transferred. Transfers of all information (including personal information) must comply with professional standards and relevant legislation (e.g. Principle 7 of the Data Protection Act 1998 which requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of, and accidental loss or destruction of, or damage to, personal data).

Source

- Great Britain (1998) the Data Protection Act 1998 The Stationery Office, London http://www.legislation.gov.uk/ukpga/1998/29/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 2011 The Stationery Office, London http://www.legislation.gov.uk/uksi/2003/2426/contents/made

- 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

- 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 http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/2010cgmanual.pdf

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

- 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
- 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

    - Royal College Physicians: Generic Medical Record Keeping Standards, https://www.rcplondon.ac.uk/resources/generic-medical-record-keeping-standards

- Department for Health The 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 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

- 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

- 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

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

- HSC ICT Security Policy

GUIDANCE

Security of Information Transfers

1. Transfers of information between an organisation's departments and sites, other HSC organisations, are commonplace and may be achieved using a variety of transfer means and formats (i.e. digital and hardcopy). It is a legal responsibility of an organisation to ensure that transfers of personal information for which they are responsible (as a Data Controller defined in the Data Protection Act 1998) are secure at all stages.

2. The loss of personal information will result in adverse incident reports which will not only affect the reputation of the organisation but, in the case of disclosing personal information intentionally or recklessly, is also a criminal offence. With effect from April 2010 fines of up to £500,000 may be imposed by the Information Commissioner's Office on organisations that do not take

reasonable steps to avoid the most serious breaches of the Data Protection Act.

Person Identifiable Information / Sensitive Information – Definitions

3. **Person Identifiable Information**. This relates to information about a person which would enable that person's identity to be established. This might be fairly explicit such as an unusual surname or isolated postcode or items of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

4. **Sensitive Information**. This can be broadly defined as that which if lost or compromised could affect individuals, organisations or the wider community. The ICO defines and provides examples of personal and sensitive data (see http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions) **All person identifiable and sensitive information** should be protected.
Secure Receipt of Personal Information

5. As well as identifying and risk assessing the routine transfers / flows of person identifiable information to and from the organisation(see para 13), there must also be procedures in place to ensure such information is received at a secure and protected point. These secure points, also referred to as safe havens should be in place wherever personal identifiable information is received, including transcribing of phone messages, fax in-trays, electronic mailboxes, pigeon holes and in-trays for paper information.

6. Access controls and registered access levels to these secure receiving points should be restricted to those who need access to the information in order to carry out their routine tasks. Where new rights to access service user information are required they should be agreed by the Personal Data Guardian or equivalent senior person with responsibility for confidentiality.

Protection for Receiving Points

7. If internal mail is being used to receive person identifiable or sensitive information, it is essential that physical security measures, e.g. key coded or swipe card entry, lockable doors / cabinets are in place to protect information in the post-room, post collection point or similar work areas.

8. Emails containing person identifiable or sensitive information must be stored appropriately on receipt, e.g. incorporated within the individual's record, and deleted from the email system when no longer needed.

Technical and Organisational Measures

9. **Accountability**. IAOs (or equivalent) should ensure that all information transfers are subject to agreed management and information security controls in compliance with the HSC IT Security Policy.

10. This is primarily aimed at the protection of personal data but will also be necessary for other sensitive information, e.g. commercially sensitive.

11. **Risk Assessments for Information Transfers**. IAOs (or equivalent) must ensure that risk assessments of proposed transfers of information are conducted, documented and appropriate safeguards are implemented to protect the information (including encryption of service user information in compliance with the HSC IT Policy). The assessment must consider the urgency, information sensitivity, costs involved and other options available. Operating procedures must be developed for secure and effective data transfer and all users made aware of their responsibilities (see also the Security Management Standard).

12. The following criteria must be considered for the transfer of information in both hardcopy and digital formats:

    - Adequate protection from interception, copying, modification, misrouting and destruction. In the case of digital information (including email file attachments) this includes protection from malicious code.

    - Documented policies, procedures and guidance which are available to users to support the appropriate use of the method of transfer, e.g. courier, post, email, World Wide Web, Intranet, wireless networks, facsimile (fax).

    - Records management, data retention, disposal requirements and guidelines.

    - Assurance measures such as physical spot checks of compliance with policies and procedures, technical monitoring of communication traffic.

    - Assurance measures, such as incident reporting analysis to evaluate the effectiveness of the security controls in place.

13. **Information Flow Mapping**. To ensure all transfers are identified the organisation must determine where, why, how and with whom it exchanges information. This is known as Information Flow Mapping and the comprehensive register provided by this exercise identifies the higher risk areas of information transfers requiring effective management.

14. Organisations should use the draft risk assessment methodology proposed by the Department in the current review of the existing mechanism to rate risks. This guidance should be formalised within the next year. The general principle of rating risks is based on likelihood and impact.

Reporting Outcomes of Information Mapping

15. Reports, highlighting data flows and all risks identified, should be provided to the organisation's IG steering group (or equivalent) with responsibility for IG issues.

16. Any significant risks (medium to high) must also be reported to the SIRO (or equivalent).

17. In some circumstances the appropriate provision of essential services may justify a degree of risk for a period, but this should be reported to, and agreed by, the Board (or equivalent) which has authority to commit the organisation to such risks. Plans must be developed for securing the information flow as soon as possible.

18. Data Access Agreements should be in place as outlined in the DHSSPS and HSC Protocol for sharing Service User Information for Secondary Purposes, with all organisations with which the organisation shares personal identifiable information for secondary purposes.

19. Any sharing of personal information for direct care purposes from one organisation to another should be in compliance with Data Protection Principle 7 which deals with the security of the transfer. Such transfers must also comply with the protocol for hospital transfer of patients and their records and the professional standards for handover and discharge of patient records.

Monitoring of Communications

20. Monitoring of communications, e.g. emails sent or received by users is subject to legislation, including the Data Protection Act 1998, the Privacy and Electronic Communications Regulations 2003 and the Regulation of Investigatory Powers Act 2000. Regulations such as Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 also impact on monitoring.

21. Monitoring emails for malicious codes or misuse is important, however, organisations should be clear what monitoring is being routinely conducted. Covert monitoring (normally used when criminal activity is suspected) is subject to the Regulation of Investigatory Powers Act. In such cases the police and the BSO Fraud Specialist must be consulted. Organisations should adhere to the legal obligations and codes of practice such as the Information Commissioner comprehensive Employment Practices Code, part three of which covers monitoring in the workplace (see extract below):

    "Workers who are subject to monitoring should be aware when it is being carried out, and why it is being carried out. Simply telling them that, for example, their emails may be monitored may not be sufficient. They should be left with a clear understanding of when information about them is likely to be obtained, why it is being obtained, how it will be used and who, if anyone, it will be disclosed to."

22. **Corporate Responsibility.** Organisations may be held responsible for the content of any messages originated by their staff. Therefore, it is essential that all national and local conditions for acceptable use, e.g. email and its implications are well defined and communicated to staff during their induction training. As public service authorities, reference to confidentiality of communications, content monitoring and freedom of information disclaimers may be advisable on external correspondence such as email.

Training

23. The HSC Leadership Centre has developed a **Regional eLearning** suite of programmes for IG. The suite of programmes will be available regionally to those organisations that make up the IG Advisory Group chaired by the DHSSPS Information Management Branch.

24. The Data Protection (DPA) and ICT Security (IT) modules are relevant to this criterion. As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of each module.
- **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:

- there are 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:

- data access agreements;
- policy/procedures
- documented plans/reports;
- information risk reports
- transfer agreements
- reports 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 Criterion

ICT Management

Risk Management

Department of Health Information Governance Toolkit Reference - 13-308

Criterion 17

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

INFORMATION

Criterion Description

A fundamental principle of the Data Protection Act 1998 is to use the minimum personal data to satisfy a purpose and to strip out information relating to a data subject that is not necessary for the particular processing being undertaken. This principle is aligned with the Caldicott Principles familiar to HSC organisations and is supported by both common law confidentiality obligations and the Human Rights Act 1998 which provides a privacy right for individuals.

Source

- 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
- Department of Health The Caldicott Guardian Manual 2010 http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/2010cgmanual.pdf
- Information Commissioner's Office Anonymisation: Managing Data Protection Risk Code of Practice November 2012 https://ico.org.uk/media/1061/anonymisation-code.pdf
- Common Law duty of Confidentiality[3] (see http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/publicationsandstatistics/publications/publicationspolicyandguidance/browsable/DH_5803173)
- 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 Your Right to Confidentiality 2012 http://www.dhsspsni.gov.uk/codeofpracticeleafletapril2012

[3] 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.

GUIDANCE

Pseudonymisation and Anonymisation

1. The Data Protection Act 1998, the Human Rights Act 1998 and the common law relating to confidentiality apply to all organisations. They require that the minimum personal data are used to satisfy any particular purpose, that organisations respect people's private lives unless there is a lawful exemption to the Human Rights requirements and that information obtained in confidence should not normally be used in an identifiable form without the permission of the service user concerned.

2. Organisations are increasingly reliant on anonymisation techniques to enable wider use of personal data. In November 2012 the Information Commissioner published the Anonymisation: Managing Data Protection Risk Code of Practice. The code explains the issues surrounding the anonymisation of personal data, and the disclosure of data once it has been anonymised. It explains the relevant legal concepts and describes the steps an organisation can take to ensure that anonymisation is conducted effectively, while retaining useful data. All organisations that turn personal data into anonymised data should use this code.

3. HSC organisations should:

    - ensure that relevant staff are aware of and trained to use anonymised or pseudonymised data;

    - ensure appropriate changes are made to processes, systems and security mechanisms in order to facilitate the use of de-identified data in place of service user identifiable data; and

    - ensure that organisations from which care is commissioned comply.

Pseudonymisation Guidance

4. The key principle is to ensure, as far as is practicable, that individual service users cannot be identified from data that are used to support purposes other than their direct care or to quality assure the care provided. Where this is not practicable data should flow through business processes that minimise the risk to data. In many circumstances this requires data to be received by a part of the organisation designated as a 'safe haven' where it can be processed securely and only used in an identifiable form for specific authorised procedures within the safe haven boundary. Onward disclosure should be limited to pseudonymised or anonymised data.

5. Effective pseudonymisation and/or anonymisation processes depend upon robust IG and effectively trained staff who understand the importance of DP and confidentiality. Where there are weaknesses in an organisation's IG its pseudonymisation and anonymisation processes are unlikely to be effective. It is not therefore possible to progress to higher attainment levels against this

requirement where requirements relating to IG management, confidentiality and DP assurance and information security assurance are not met.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- there is a clear plan for protecting the confidentiality of service user information by using appropriate pseudonymisation and anonymisation methods for purposes other than direct care.

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

- robust IG processes have been established to support the implementation of the pseudonymisation/anonymisation plan.

- business processes are reviewed to ensure that the organisation remains compliant with the requirements to protect the confidentiality of service user information.

Examples of evidence include:

- policy/procedures
- documented plans/reports;
- reports 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 - 13-324

Criterion 18

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

INFORMATION

Criterion Description

The HCN is the regional unique service user identifier in operation in the HSC. Using the HCN makes it possible to share service user information safely, efficiently and accurately across HSC and partner organisations.

Source

- 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 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

- DHSSPS HSC (SQSD) 15/2008 Standardising wristbands improves patient safety http://www.dhsspsni.gov.uk/hsc__sqsd__16-08.pdf**Managing Public Money NI A3.1 : Governance Statement http://www.dfpni.gov.uk/index/finance/afmd/afmd-key-guidance/afmd-mpmni/a.3.1_governance_statement.pdf**

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

- DHSSPS HPSS ICT Programme, From Vision to Reality, March 2005 https://www.dhsspsni.gov.uk/publications/hpss-ict-programme-strategy-march-2005

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

GUIDANCE

In order to ensure safer practice in acute, community and social care settings, general medical services and regional screening services HSC organisations and practitioners are required to:

1. Use the HCN as the regional service user identifier; or alternatively, the HCN as the regional service user identifier in conjunction with any other local

administrative numbering system (i.e. where local numbers are used they must be used alongside and not instead of the HCN).

2. Use the HCN (and its barcoded equivalent) in/on all correspondence, notes, /service user wristbands and /service user care systems to support accuracy in identifying service users and linking records.

3. Put processes in place to ensure that service users identify themselves in a consistent manner. Until further guidance on protocols to be used in this regard is issued for consultation, as a minimum, service users should be asked for their formal Forename(s)/Surname and their date of birth as it appears on their birth certificate.

4. These actions, as set out in SQS Learning Communication 05/09, will help in deciding whether the key requirements of this criterion are being met.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- a plan is in place to support the consistent and comprehensive use of HCN in line with S&Q Learning Communication 05/09.

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

- all retrospective and future HSC Demographics Improvement Group feedback reports are addressed.

- progress / highlight reports, in line with local governance arrangements are reported to the Organisation's Board.

Examples of evidence include:

- named individuals' job descriptions;
- documented plan;
- description of the demographic data quality function;
- 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

Risk Management

Department of Health Information Governance Toolkit Reference - 13-401

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

INFORMATION

Criterion Description

Staff must be provided with procedures for collecting and accurately recording service user information on all systems and/or records that support the provision of care, and for routinely checking information with the source. The procedures must be monitored and where errors are identified, for example duplicate or confused records, corrections should be made.

Source

- Great Britain (1998) the Data Protection Act 1998 Principle 4 The Stationery Office, London http://www.legislation.gov.uk/ukpga/1998/29/contents
- Northern Ireland: HPSS: The NI Data Dictionary http://hscb.sharepoint.hscni.net/sites/pmsi/isdq/SitePages/DataDictionary.aspx
- Good Management Good Records 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
- Audit Commission: Data Remember - Improving The Quality of Patient-Based Information 2002 http://archive.audit-commission.gov.uk/auditcommission/sitecollectiondocuments/AuditCommissionReports/NationalStudies/dataremember.pdf

Guidance

Accurate Collection and Recording and of Service User Data

1. High quality information means better care and safety. If service user information is inaccurate, there could be consequences for care, treatment and safety, for example, there could be problems in contacting that service user to arrange a necessary appointment/meeting. The service user could then experience significant delays in receiving essential treatment or care.

2. All those involved in the care of an individual need to be able to rely on the accuracy of the available information in order to be able to provide timely and effective treatment or care for that individual. To maintain the integrity of service user information and to minimise risk, organisations should have procedures in place for the collection of service user information and for checking the information held on all systems and/or in health/care records that support the provision of care with the source. The source will usually be the

service user themselves (or their guardian), or may be their notes or clinical/care correspondence.

Staff Procedures and Training for Data Collection and Recording

3. Procedures for the collection and recording of accurate and complete information wherever the collection occurs should be in place throughout the organisation. These will include procedures for staff and procedures to ensure synchronicity between databases - see **paragraph 20**.

4. Where necessary, procedures should be documented for:

   Admission - covering all departments, wards and areas where service users are admitted for emergency assistance, elective admission;
   Outpatient or office visits - covering all locations where clinics or pre-arranged meetings are, booked and/or held and where service users are seen for a day time appointment;
   Home visits - covering community staff and the way they collect information from service users and transfer it to systems supporting the provision of care;
   Other areas in the organisation - where there is a system that will need updating when new information is received, e.g. A&E, Pathology, Housing department.

5. Procedures on the collection and recording of accurate data should be made available to all relevant staff and copies of the documentation should be kept close to where the procedures are being carried out, so that staff can easily refer to them. Where service user information is captured in the community setting staff must have procedures that they can access easily. This may be in the form of a portfolio of procedures which staff can keep with them whilst working within the community.

6. Staff should be informed of the procedure (see para 13) to report an error or omission within a record they are handling, so that timely improvements to information quality can be made and training gaps or weaknesses can be identified.

7. All staff should receive training and awareness sessions to ensure that they understand the importance of collecting and recording accurate service user information to minimise the risks to the service user and to the organisation itself. The use of examples and scenarios may be particularly useful to ensure that a basic level of competence has been achieved before access to the systems is allowed.

8. The training programme must cover all aspects of information quality required:

   - the definition of individual data items - so that staff know what they are recording;
   - the eventual use of data – so staff understand what the data they are recording will eventually be used for (and therefore why it is important to record accurately);

- the function of data items – so staff know the purpose of recording;
- how to validate data with the service user or against the health/care record – so checks are carried out to confirm the accuracy of data.

9. Organisations must ensure that no staff members are able to use or enter data onto systems supporting the provision of care, without adequate training. This must include temporary, locum and clinical/care staff.

10. All staff that collect service user information are responsible for checking that the data is accurate, complete and entered into the system appropriately and efficiently.

11. The training programme should be monitored and regularly reviewed to ensure that training materials and guidance are kept up-to-date.

Verifying Service User Information

12. People accessing services should be given opportunities to check information held about them and be allowed to point out any mistakes. Service users should be encouraged to provide the information themselves rather than staff 'checking' information already held. The most effective way of doing this would be for example asking the service user 'can you tell me your full address' or 'Can you tell me who your GP is'. Asking the service user to provide the address details means they will provide the most up-to-date information, rather than saying 'yes' to being at the same address which may be incorrect/out of date on the system. This best practice method should be covered in a staff procedure document/sheet. Organisations should include advice about the importance of providing of accurate information in their information leaflets, posters and other materials.

13. The organisation should put processes in place that direct staff to report and/or take appropriate action when factual errors in health/care records are identified as soon as is reasonable. The action to be taken will depend on the type of record (i.e. paper or electronic) and should take into account legislation (e.g. the Data Protection Act 1998) and guidance on deletions or corrections in service user records.

14. Checks on the accuracy of service user information should occur whenever the service user presents or where their records are being updated, for example:

- whenever a service user attends an appointment;
- if a service user rings a call centre for booking appointments;
- whenever referrals are received;
- on admission (for secondary care services or treatment).

Amendment to record

15. Staff members need to understand what the options are and how to respond sensitively to concerns raised by service users. If an individual is unhappy about an opinion or comment that has been recorded, they have the option to have their comments added to their record. Additionally, if a person is suffering distress or harm because of information held in their record, they can apply to have the information amended.

Consequences of Inaccurate, Incorrect, Duplicate and Confused Records

16. Failure to adhere to procedures for the collection and recording of accurate information may lead to the creation of inaccurate, incorrect, duplicate or confused records.

17. Duplicate records maybe created when:

- the same individual is registered more than once on a HSC system. Although many systems will stop exact matching duplicates, there continue to be systems which allow multiple matching duplicates to be created.
- the same individual is registered on different systems at the same organisation, which are not interfaced and therefore there are different records for different aspects of treatment. These of course can lead to the production of duplicate records if and when these two systems are merged;
- the same individual is registered on different systems which are interfaced and therefore more than one record is available at any point in their treatment.

18. The organisations method for dealing with duplicate records should be clearly covered within a staff procedure document/sheet so that staff have a clear understanding of what they need to do to report/deal with duplicate registrations.

19. Confused records are created when information relating to two or more service users is included within one record.

Other Causes of Duplicate or Confused Records

20. A number of duplicates or confused records can occur where service users have the **same** Forename, Surname, Date of Birth, and Postcode. Common data entry errors that can contribute to the creation of duplicate or confused health/care records include:

- individuals with the **same** Forename, Date of Birth and Postcode, and where the first three letters of the Surname is also the same;

- individuals with the **same** Date of Birth, Postcode, and Surname, and where the Forename **initial** is also the same;

- individuals with the **same** Surname, Forename and Postcode, and, **two** out of **three** elements of the Date of Birth are the same;

- mis-association of a data item where only one of the following data items differs - Forename, Surname, Date of Birth and Postcode.

Reconciling Service User Information

21. Where different systems that support the provision of care maintain common sets of demographic data, there should be documented procedures for maintaining synchronicity between the separate databases and for reconciling any differences. This may be a manual or automated process.

22. These procedures are designed to get organisations to look at their systems (i.e. these systems would not include retrospective audit systems) and to ensure that common data is updated in a timely manner across them as more up-to-date information becomes available. Where systems share an interface and update each other then this should not be a problem.

23. Staff members that introduce new systems to support the provision of care must also ensure that data collection, data quality, synchronicity and duplication issues are considered within the planning process - see also the IT standard.

24. Any updates in systems on the basis of reliable new information (particularly in relation to demographics), should be replicated in the other systems. For example, where a service user notifies a change of address this should feed through to other systems, to ensure that future correspondence does not go astray. Ideally this should be done automatically through fully integrated systems.

25. Where information is captured that is not linked through to other systems, procedures are required to ensure that the all other systems are routinely updated appropriately. That is all systems that support the provision of care. Operational systems should be as up-to-date as the organisation can reasonably make them.

26. The procedures for reconciling service user information should reflect that:

- appropriately trained staff amend the system(s) and paper records if a service user's details have changed;
- all staff must have an understanding of the importance of making amendments and the implications of failing to do so, including possible adverse impact upon the service user (e.g. urgent appointments going to the wrong address);

- routine audit and monitoring is undertaken to ensure the procedures and processes in place for checking and correcting service user records are effective.

Monitoring Data Collection Activities

27. Responsibility for monitoring data collection activities should be assigned to appropriate individuals, whose primary role is to ensure the accuracy of data held in service user systems. These responsibilities should be included in job descriptions that are regularly reviewed, and identified within performance appraisals.

28. There may be several different procedures that are required for the robust monitoring of data collection activities, all of which should be in line with other information quality procedures used in the organisation.

29. The Trust may produce a number of data quality monitoring reports that cover all aspects of quality in relation to care and treatment. For the purposes of this requirement a report(s) simply needs to cover the quality of service user demographic data and the numbers of duplicate registrations, for example: Percentage completion of name, address, date of birth, H+C Number, registered GP and numbers of duplicate records.

30. Monitoring activities will also include spot checks to assess whether all staff members are complying with the data collection procedures, and identify any areas for improvement.

31. Organisations should produce, analyse and use missing data reports to identify the causes of missing or incomplete data and take appropriate corrective action.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- there are documented and approved procedures to ensure the accuracy of service user information on all systems and/or records that support the provision of care.

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

- data collection and validation activities are regularly monitored. All staff collecting and recording data are effectively trained to do so and dedicated staff take appropriate action where errors and omissions are identified

- regular audits and reviews are carried out to monitor the effectiveness of data collection and validation activities.

Examples of evidence include:

- named individuals' job descriptions;
- policy/procedures
- documented procedures
- training materials
- reports 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

Governance

ICT Management

Department of Health Information Governance Toolkit Reference - 13-402

Criterion 20

A multi-professional audit of clinical and social care records across all specialties has been undertaken

INFORMATION

Criterion Description

It is essential that organisations undertake audits of clinical and social care records in all specialties to ensure that the quality of the health/social care record facilitates high quality treatment and care and that subsequently a health/social care record can justify any decisions taken if required.

Source

- 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

- The Royal College of Physicians Generic multidisciplinary clinical record keeping standards: audit tool May 2011 https://www.rcplondon.ac.uk/resources/generic-multi-disciplinary-clinical-record-keeping-standards-audit-tool
- Royal College of Physicians A Clinicians guide to Record Standards part 1 and part 2 October 2008 https://www.rcoa.ac.uk/sites/default/files/FPM-clinicians-guide1.pdf
- Evidence on the quality of medical note keeping: guidance for use at appraisal and revalidationhttps://www.rcplondon.ac.uk/guidelines-policy/evidence-quality-medical-note-keeping-guidance-use-appraisal-and-revalidation
- 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 (PRONI) – Northern Ireland Records Management Standard https://www.nidirect.gov.uk/articles/records-management-public-bodies
- General Medical Council: A-Z of guidance/record keepingGreat Britain (1998) the Data Protection Act 1998 The Stationery Office, London http://www.legislation.gov.uk/ukpga/1998/29/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

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

- 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 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

- Social care governance: A practice workbook for Northern Ireland Second edition published: April 2013

- British Medical Association : Guidance for Health Professionals in the UK December 2008 http://bma.org.uk/practical-support-at-work/ethics/confidentiality-and-health-records
- NMC Record Keeping guidance for nurses and midwives July 2009 http://www.nmc-uk.org/Documents/NMC-Publications/NMC-Record-Keeping-Guidance.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

Auditing Clinical Records

1. Accurate records are essential to support high quality treatment and care. Inaccurate records can lead to delays to service users receiving treatment, inappropriate care and duplicate records, which all present a risk to the service user.

2. Clinical **and social care** records are among the most basic of tools which are used in almost every consultation, providing an accurate picture of the care and treatment given to an individual, and assist in making sure they receive the best possible care. They also aid effective communication with other healthcare professionals.

Standard Design for Records

3. Clinical and social care records should have the following key features:

    - made of durable material with secure anchorage points;

- a mechanism to secure machine tracings, e.g. cardiotopography, electrocardiography, electro-encephalography, to the body of the folder;

- locally agreed standard format for filing within the folder with an index with clear instructions for the filing of documents in each section and the order in which they are to be filed;

- operation notes and other key procedures should be readily identifiable;

- a designated place for the recording of hypersensitivity reactions and other information relevant to all healthcare professionals;

- viewable in chronological order so that they can reflect the patient's experience of healthcare and reflect the continuum of service user care.

Record Keeping Standards

4. A number of professional bodies and regulators (for example the Royal College of Physicians the Nursing and Midwifery Council and the Northern Ireland Social Care Council) acknowledge the importance of accurate records to the delivery of safe and effective care and treatment, and have issued guidance around good record keeping for clinicians, nurses and other health and social care professionals.

5. An audit of the accuracy of record keeping should be focused on the following criteria:

    - **Legibility**: All entries into the record, including amendments should be clearly written in black ink. If another colour ink is used (e.g. to identify a specific alert for example penicillin allergy) this should be agreed and documented by the Health Records group and all staff should adhere to it.

    - **Attributability**: All entries into the record, including amendments should:

        - be clearly dated, timed, signed;

        - clearly record the designation of the person making the entry.

      Copies of signatures of all professionals who make entries in the record, and where appropriate their professional registration number, should be retained by the organisation as directed in GMGR. Contracts of employment for all clinical and social care staff should include clauses on the importance of good record keeping to ensure

that staff are aware of the responsibilities and that their compliance with the procedures will be monitored.

- **Timeliness of entries**: All entries should be made contemporaneously (i.e. at the same period of time) whenever possible or made immediately after the service user/clinician/professional contact.

6. Organisations should have a procedure in place for logging queries from internal sources about entries in the record. This procedure is to enable staff to raise a query if they identify an error or anomaly within a record they are handling, i.e. the identification of errors/anomalies outside of any issues discovered by more formal audit processes. The purpose is to make timely improvements to information quality by providing a record of quality issues for review and correction and identifying training gaps or weaknesses. The method of logging such queries is a local decision, but for example, queries could be incorporated within existing incident reporting mechanisms or there could be a hard copy or email template.

7. The Royal College of Physicians (RCP) has defined 12 generic record keeping standards as part of a programme for establishing professional standards for all components of medical records. These are practical, commonsense standards that can be applied to any service user's health records.

8. Midwifery and machine records (e.g. foetal heart monitors) should be written and filed in chronological order.

Auditing Service User Records

9. An audit should help your organisation identify areas where practice could be improved. This may include not only changing policies and procedures but also changing behaviours throughout the organisation and providing additional guidance and training.

10. Audits should be undertaken in high risk specialties for example intensive care, coronary care/surgery, high dependency, child protection.

11. The Royal College of Physicians has developed an audit tool based on the generic record keeping standards which have been approved by the Academy of Medical Royal Colleges in April 2008. This tool could be used by organisations to supplement and support the work that is already being undertaken around record keeping.

12. For this requirement the audit must have been conducted within the twelve months prior to the final controls assurance standard submission.

Training

13. All health and social care professionals who use or are responsible for records should be trained to ensure that they are aware of the locally agreed

standard format for filing within the record, the record keeping standards to be followed, the importance of accurate service user identification and that they understand their responsibilities in relation to record keeping.

14. The HSC Leadership Centre has developed a **Regional eLearning** suite of programmes for IG and will be available regionally to those organisations that make up the Information Governance Advisory Group chaired by the DHSSPS Information Management Branch. The Records Management (RM) programme is relevant to this requirement

15. 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:

- their approach to auditing clinical and social care records has been documented and a procedure is in place for logging queries from internal sources about entries in the record.

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

- the approach to auditing clinical and social care records has been implemented and all staff are informed of their responsibilities with regards to clinical record keeping.

- an audit of clinical and social care records has been completed for professional groups across all specialties (including maternity services where these are provided) with audit results being fed back to health and social care professionals and actions taken to improve/maintain performance.

Examples of evidence include:

- documented procedures;
- training and induction materials
- audit reports;
- 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 - 13-404

Criterion 21

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

INFORMATION

Criterion Description

Effective records management requires that an organisation is able to identify locate and retrieve information when and where it is needed. To support this, there must be effective procedures in place for monitoring and measuring paper health/care record availability.

Source

- Great Britain (1998) the Data Protection Act 1998 Principle 4 and 7 The Stationery Office, London http://www.legislation.gov.uk/ukpga/1998/29/contents

- DHSSPS Controls Assurance Information Management Standard June 2012 http://www.dhsspsni.gov.uk/governance-controls

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

- Department of Health Core and Developmental Standards C9 http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/Browsable/DH_4894544

- 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

Monitoring the Availability of Paper Health/Care Records

1. Even with the drive toward electronic care records, organisations will be reliant on paper records to record and review the delivery of care for some years to come. It is important that these records are available when and where they are required so that care and treatment can be effectively provided based on the most up to date information.

2. Organisations should therefore put measures in place to support identification and retrieval of records to ensure that a service user's complete record is available when it is required. The procedures should be in line with the principles contained in Good Management Good Records.

Storage of Paper Records

3. In the first instance, there should be appropriate storage arrangements for records that are not currently in use, e.g. a records library. This area should be made known to all staff using paper records so that records are not stored inappropriately in offices or filing cabinets where authorised users cannot gain access when required.

4. Access to the storage arrangements should be to authorised staff only and allow for the retrieval of paper records when they are required. The environment of the records storage area must also be monitored to ensure that it is not at risk of flooding and protected as much as possible from other hazards such as fire.

5. In HSC secondary care organisations this retrieval should be provided by trained records staff on a 24 hour / 7 day per week basis.

Monitoring Health/Care Record Availability

6. Procedures for monitoring the availability of paper health/care records should include measures to track records within the organisation, for example a tracking log that sets out when records are removed from the storage area, where they were transferred to, by whom and when they are returned. In many HSC organisations barcode scanners are used, (and casenote tracking modules within electronic Patient Administration Systems) to track records in and out of departments within the organisation, this will make tracking logs more accurate and effective in the monitoring of availability.

7. Procedures should also cover the disposal of records, migration to other media and transfer to other authorised organisations including off-site storage locations.

8. Specific guidance should be provided to community staff; the guidance should emphasise information security and confidentiality and set out additional information to be recorded in the tracking log when records are taken offsite, e.g. the purpose, and when the record will be returned.

9. A log should be kept of all missing paper records and measures should be in place to trace these records. The log should clearly state the location where a record was last seen and any actions taken to find it. Missing files can also lead to duplicate and confused records, for further guidance on this area see **criteria 19**.

Reporting

10. The reason for non-availability of records should be clearly documented and reports on record availability should be reported to the IG forum, a records management group, or similar, at regular intervals.

11. Appropriate management action should be taken, which dependent on the reason for non-availability might be updating the procedures for tracking and tracing, implementing new security measures, staff re-training, disciplinary measures etc.

12. A senior manager with responsibility for information risks, e.g. the SIRO should receive prompt reports where there is widespread non-availability of records, e.g. due to a fire or flooding in the storage area.
13. Where the number of non-available records is consistently high this should be included within the risk register or similar for consideration by senior management.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- there are documented and approved procedures to monitor the availability of paper health/care records, including tracking records and tracing missing records.

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

- the procedures for monitoring the availability of paper health/care records have been implemented and action taken where availability of records is considered poor.

- staff compliance checks are routinely undertaken to ensure staff are following the record tracking process and appropriately reporting unavailable or missing records.

Examples of evidence include:

- written procedures;
- 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 - 13-406

Criterion 22

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

INFORMATION

Criterion Description

Organisations should ensure that all service user information systems incorporate national data definitions, standards and values where these exist, and key electronic systems have validation programmes built in that are conformant with, or map to these national standards. These should be kept up to date and audited and local systems documentation should be updated as standards develop.

Source

- Northern Ireland: HPSS: The NI Data Dictionary
  - http://hscb.sharepoint.hscni.net/sites/pmsi/isdq/SitePages/DataDictionary.aspx
- DHSSPS guidance on Statistical Information Returns http://dhsspsextra.intranet.nigov.net/index/statistics.htm
-
- Great Britain (1998) the Data Protection Act 1998 Principle 4 The Stationery Office, London http://www.legislation.gov.uk/ukpga/1998/29/contents

GUIDANCE

National Data Definitions, Values and Validation

1. National definitions and guidance support the sharing, exchange and comparison of information across the HSC. Common definitions, known as data standards, are used to support comparative data analysis, for the preparation of performance tables, and for data sharing and also support clinical messages, such as those used for pathology and radiology.

2. National data standards should not just be seen as supporting the collection of data on a consistent basis throughout the HSC. They also have an important role in supporting the flow and quality of information used, so that care professionals are presented with the relevant information where and when it is required to provide effective care and treatment to service users.

National Standard Definitions, Values and Validation Programmes *This requirement applies in full to key electronic systems*

3. Organisations should ensure that:

- electronic systems have built in validation programmes which are conformant with, or map to national Data Standards (where these exist);

- for the relevant service user information systems, where national data standard definitions and values exist, these definitions and values are used:

- values on the key systems Master Files match the national standard definitions where these definitions exist;

- any proposed changes to national standard definitions and values, including their interpretation and application, are agreed centrally through the pre-agreed mechanisms before being implemented;

- no other values are used unless these are mapped explicitly to national data standard definitions and values (where these exist) for central returns;

- the number and combination of alpha/numeric digits within a code match the format of the Data Dictionary and the code conforms or maps to a nationally determined coding structure.

4. Codes and validation programs must be kept up-to-date, and cannot be switched off or overridden by operational staff. Regular audits should be undertaken to ensure that errors are identified and acted upon.

5. Organisations must designate responsibility for ensuring that systems are kept up-to-date in the light of developing national guidance and standard definitions, and ensure that this responsibility is written into an individual's job description.

6. Organisations should also have policies/procedures for checking:

- duplicate records, which should be monitored and reviewed regularly. ‘Duplicate Records’, for the purposes of this requirement, means duplicate care records (see **Criteria 19**) and duplicate episodes;

- validation programmes are used routinely on data entry, and completeness and validity of data sets, both those used locally and for central returns;

- standard definitions against the Master Files on key systems, by checking all the Master Files relating to these definitions against national definitions and codes;

- validation routines (possibly using fictitious service users if this is appropriately controlled).

7. The Department is working with the HSC Board, Trusts and PHA through the Regional Information Group (RIG) and its four subgroups: the Data Information Standards/Data Quality Sub Group, Community Information Sub Group, Acute Sub Group and Clinical Coding Sub Group to improve data definition standards. Organisations should ensure Data Definition Standards etc. are developed in line with the RIG programme of work.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- all key service user information systems incorporate national HSC and/or social care definitions and values.

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

- service user information systems have validation programmes built in that are kept up-to-date and cannot be switched off or overridden by operational staff. All documentation for local systems is regularly reviewed and updated appropriately as standards develop.

- validation programmes are regularly tested to ensure that errors are identified and acted upon. The effectiveness of the arrangements for updating local documentation is regularly reviewed in conjunction with appropriate stakeholders.

Examples of evidence include:

- named individuals' job descriptions;
- system design or outputs ;
- communications with staff;
- audit reports
- 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 - 13-501

Criterion 23

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

INFORMATION

Criterion Description

Data quality reports from external organisations should be used to monitor and improve data quality and take any necessary actions to ensure that issues are followed up and resolved.

Source

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

GUIDANCE

Monitoring and Improving Data Quality

1. Service user care and safety depends on good quality data. Poor quality data can impact on care, damage the reputation of organisations and individuals, lead to flawed clinical/care, administrative and planning decisions, and disrupt funding.

2. Organisations can assess and ensure the quality of their data by:

    a. using a series of monthly quarterly and annual error reports;
    b. accessing data quality reporting tools;
    c. investigating external data quality reports.

3. For this requirement, external sources are those organisations to which data or returns are sent, which are external to the organisation, for example:

    a. The Health and Social Care Board;
    b. Other HSC organisations
    c. General Practitioners;
    d. Department of Health Social Services and Public Safety;
    e. Business Services Organisation (BSO).

4. For this requirement, organisations must have evidence that data quality reports or queries on its data from external sources are received and logged, and that they are actioned appropriately.

5. Procedures must be in place to ensure that data quality reports on the organisation's data from external sources are followed up and appropriate

corrections made, with an effective feedback loop to staff to help prevent similar mistakes being made in future.

6. The Board/senior management or delegated sub-committee/group should be kept aware of progress. Action plans for improvement should be signed off by the delegated sub-committee/group or senior management, and appropriate resources will need to be applied to ensure the success of these.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- a process has been developed for using external data quality reports for monitoring quality.

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

- data quality reports from external sources are followed up and appropriate corrections made. Reports on data quality are shared with the Board/senior management team or delegated sub-committee/group.

- improvement plans have been developed for improving data quality and signed off by the information manager/senior management team or delegated sub-committee/group and appropriate resources have been allocated for improvements to be made.

Examples of evidence include:

- named individuals' job descriptions;
- processes and procedures ;
- communications with staff;
- improvement plans
- training programmes
- 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 - 13-502

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

INFORMATION

There are established procedures in place for the regular assessment of clinical coding. The results of any clinical coding audits conducted within the last twelve months based on the requirements and standards within the NHS Classifications Service Clinical Coding Audit Methodology are noted and actioned. Audits are undertaken by an NHS Classifications Service approved clinical coding auditor.

Source

- Great Britain (1998) the Data Protection Act 1998 Principle 4 and 7 The Stationery Office, London http://www.legislation.gov.uk/ukpga/1998/29/contents

GUIDANCE

Robust Data Quality and Clinical Coding Audit Programme

1. Clinical coding staff depend on clear, accurate information in order to produce a true picture of hospital activity and the care given by clinicians. Coded data is important for a number of reasons, for example:

    - monitoring provision of health services within Northern Ireland;
    - clinical governance;
    - research and monitoring of health trends.

2. The NHS Classifications Services provides a working model for carrying out coded clinical data audits.

Audit Programme – Data Quality (Clinical Coding)

3. Data Quality Audit, focused on clinical coding, is a crucial part of a robust assurance framework. Organisations should implement the following:

    - A programme of clinical coding audits focused on data quality in accordance with the guidance set out below.

    This programme may be in the form of, either:

    i. a continuous clinical coding audit programme comprising several small audits undertaken throughout the course of the year as part of routine maintenance of standards (see also 12b);

    or

    ii. a series of specific clinical audits.

4. A clinical coding audit programme plan detailing what audits are going to take place in the 2016/17 year must be submitted to the Department for consideration and to elicit the Department's view on areas that it wishes to see included in the programme. The findings and recommendations from the coding audits should also be submitted to the Department.

Data Quality (Clinical Coding) Audit Specification

5. For the purposes of this requirement clinical coding audits are performed as part of a continuous data quality programme. The audits must be based on the most recent version of the NHS Classifications Service Clinical Coding Audit Methodology and be undertaken by an NHS Classifications Service approved clinical coding auditor. There must be documented evidence that recommendations made in previous clinical coding audits have been noted and actioned.

6. Organisations should routinely undertake audits of their data as part of good practice in keeping under review their performance in providing good quality data.

7. Staff within the HSC Service in Northern Ireland are required to adhere to standards of clinical coding as agreed between the Department and the HSC Board. It is for the HSC Board to communicate and performance manage such standards with Trusts.

8. Organisations should refer to the detailed guidance provided in the NHS Classifications Service Clinical Coding Auditor Code of Conduct.

The NHS Classifications Service Clinical Coding Audit Methodology

9. Organisations should ensure they have established documented procedures in place for the audit of coded clinical data. In order to monitor the quality of coded clinical data, organisations should ensure that there is a procedure for regular audit and review.

10. The Clinical Coding Audit Methodology describes the full range of analyses that are carried out on all diagnosis and procedure codes. These include analysis of both primary and secondary diagnosis and procedure codes, for:

    - correct and incorrect codes;
    - incorrect sequencing of codes;
    - irrelevant codes and omitted codes.

    The coding audit also examines the process undertaken for coding and the documentation available for use during the coding process.

11. Selection of the sample for the audits may be informed by the results of national benchmarking and/or previous audits. Other examples include clinical specialty specific audits or a general sample which is representative of the case-mix, specialty and type of admission of the organisation, and the clinical coding auditors have a responsibility to satisfy themselves that the sample is random within this constraint.

12. For clinical coding audit the requirements for achieving substantive compliance for clinical coding analysis within Information Quality Assurance are that:

    a. Organisations should have carried out a clinical coding audit programme within the last twelve months* prior to submission of the Information Quality Assurance scores for this criteria. This may be either part of a process of continuous clinical coding audit, or, a one-off audit. This should have complied with the requirements and standards within the latest version of the NHS Classifications Service Clinical Coding Audit Methodology.

    b. The auditor must be an NHS Classifications Service approved clinical coding auditor, and must have adhered to the Clinical Coding Auditors Code of Conduct.

    c. The organisations Clinical Coding Audit Report should contain within an analysis of reasons for the errors identified, which distinguish between coder and non-coder error. For example whether the error is due to the incorrect code assigned or due to problems with documentation or process not being fit for purpose. However, for the purposes of Information Quality Assurance, an error due to either cause would be regarded as an inaccuracy. Organisations are urged to note that many issues with clinical coding may arise not from the coders, but from problems with the information given to the coders to code from, and that these will need to be addressed.

    d. Organisations should use the analysis contained in their clinical coding audit reports to understand the reasons behind any errors and that any recommendations made in the previous clinical coding audits have been noted and actioned.

    *** The 'last twelve months' is defined as between the 1st April 2015 and 31st March 2016 (inclusive)*.**

Evidence demonstrating Compliance

For substantive compliance Organisations should evidence that:

- a clinical coding audit programme plan detailing what audits are going to take place in the 2016/17 year has been submitted to the Department.

- the clinical coding audit programme has been undertaken, with full consideration of the clinical coding standards as agreed between the

Department and the HSC Board, by a NHS Classifications Service approved clinical coding auditor who has adhered to the Clinical Coding Auditor Code of Conduct within the last twelve months.

- the outcomes of all audits have been sent to the Department.

- any recommendations made in previous clinical coding audits have been noted and actioned.

Examples of evidence include:

- audit programme plan;
- policy/procedures;
- improvement plan
- audit report sent to the Department;
- 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 - 13-505

Criterion 25

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

INFORMATION

Criterion Description

Organisations should have procedures and a regular audit cycle to check the accuracy of service user data. The results of the audits should be reported as part of the organisation data quality reviews to the Board. Accuracy checks should form part of the IG Policy and be reflected in the Terms of Reference of an Information Quality Group (or equivalent group/committee).

Source

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

- Audit Commission: Data Remember - Improving The Quality of Patient-Based Information 2002 http://archive.audit-commission.gov.uk/auditcommission/sitecollectiondocuments/AuditCommissionReports/NationalStudies/dataremember.pdf

GUIDANCE

Effective Audit Cycle for Accuracy Checks on Service User Data

1. The accuracy of data is a key element of information quality which is tested through the Information Quality Assurance process. The traditional method of checking the accuracy of electronic records is against the health record.

2. However, it is recognised that in a number of organisations, health records are no longer the primary source of data for a number of data items. Information Quality Assurance has been designed to be flexible enough for individual organisations to respond to the particular situation within their organisation.

Accuracy of Data

3. The increasing use of electronic records and the implications for health records as a primary source of information have to be recognised, as does the increasing role and right that service users have to understand and influence the information held about them.

4. There are therefore four main elements for checking accuracy of data:

- checking against the health record;
- checking with external systems;
- checking items with service users (see **criteria 19**);
- checking the process for information capture.

5. For most organisations, in the majority of the checked fields, the accuracy checking process will use the health record as the prime check of electronic data accuracy. This will be done by comparing the key data item from the service user's health record with the same data item within the extracted information.

6. Where organisations already use a tried and trusted system of checking data accuracy retrospectively with samples of service user health records, then the results of these checks can also be used as evidence for accuracy, as can other recent independent audit checks.

7. Where an organisation has made a specific formal statement, minuted as agreed by its Board (or delegated sub-committee) and supported in its policy documentation, that its health records are not a primary source of data for a particular data item, and the above alternate methods of checking are not available or applicable (such as for start and end dates etc), then a detailed check of the processes for collection of that data item, focussing on evidence of the accuracy of the collection of that data (through spot checks etc), and regular audit, will be accepted.

8. The onus will be on the organisation to supply evidence to prove the accuracy of this data. Each organisation will have different processes and procedures in place which make it inappropriate to have a common definitive source for all data items collected. However, each organisation should decide the method of approach it wishes to employ for each data item and document this as part of their evidence for Information Quality Assurance.

An Audit Cycle for Accuracy Checks

This requirement must have been completed on data relating to the financial year April 2016 to March 2017

9. Organisations must ensure that there is a documented procedure and a regular audit cycle on care data. Organisations are encouraged to audit all datasets.

Health Record Checks Against a Sample of Data

10. Where the health record is the primary source of data, the accuracy assessors should select for examination a random sample of data which covers all specialties. The recommended sample size is 0.5% of records processed in the year in each data group with a minimum of 20 records being checked.

11. The aim of this requirement is to ensure that an organisation can demonstrate to itself that it is maintaining accurate information about its service users. Organisations are encouraged to audit more than the minimum set out above to provide this assurance.

12. These sample checks can be spread throughout the year in whatever way best suits the organisation. Evidence of sample size should be included in the Information Quality Assurance submission, and any inability to access the full sample may be an issue for further investigation.

Suggested Approach

13. A database, spreadsheet or printout of the selected Commissioning Data Sets (CDS) could be produced from the computer system listing the key data items to be analysed, and the corresponding random sample of health records. The list of records to be "pulled" should be provided in the order that best suits the local filing system.

14. Using data from the health record, a member of the accuracy checking team should re-code the key data items and enter the codes on a pro forma. Another member of the accuracy checking team should then examine the key data items on the CDS and write the codes on the pro forma. The two codes are compared and mismatches identified. Reasons for errors must be identified and recorded.

15. Where the data item is not specifically recorded in the health record the following may apply, and the assessor will need to apply judgement as to the action to be taken:

    - The field may by local arrangement be filled in with a default code (such as a Management Intention of Day Case for a procedure such as 'Cataracts',). Where this is the case, then a written policy / procedure should exist stating how the default will be operated. If such a policy / procedure does not exist then all the appropriate records for this data item should be regarded as 'inaccurate' for the purposes of scoring. If such a policy / procedure exists and is correctly applied in each case, then the appropriate records should be regarded as 'accurate' for scoring purposes. However, allowing default codes can lead to coding being inaccurate and this practice should only be used if absolutely necessary.

    - Some records, particularly for outpatients, may contain data items appertaining to events that occurred several years ago, such as Referral Request Received Date for an Outpatient Referral that could be several years old, with no date stamp on the referral letter. In each such case the assessor will need to exercise judgement as to whether the record should be excluded from the accuracy calculation for that data item. Although it is difficult to be prescriptive, a 3 year 'rule-of thumb' may be used with caution in some such cases.

16. The accuracy check is looking for major discrepancies and errors. It is not concerned with minor differences of interpretation. For instance, if a check of the health record reveals that a service user was admitted as an emergency, then recording of an elective code in the data would definitely be inaccurate. If however, it is unclear in the notes as to the exact method of emergency admission then the assessor may exercise some limited discretion.

Accuracy of Externally Checked Items

17. Health+Care Numbers (HCN) should be obtained and/or frequently checked through the HSC Demographics Service (part of the Business Service Organisation) or by accessing HCN Web View or other system HCN search interfaces. HCNs which have been traced and verified through the HSC Demographics Service must be regarded as accurate.

18. At this time the accuracy check for HCNs on HSC PAS is undertaken via the reports supplied to Trusts by the HSC Demographics Service with other HSC systems being included in future plans. There do exist a set of service users where rigorous checks have been undertaken which prove that the service user genuinely does not have an HCN (e.g. certain military personnel) and these should be taken account of.

19. Organisations must have adequate and timely procedures in place for the tracing of HCNs. Evidence will be required that the organisation is using adequate procedures to check the HCNs on their system.

Postcode of Usual Address

20. HSC organisations should have a process in place to verify the service user's postcodes, and should sample check a minimum of 30 records to ensure that the record matches the appropriate source.

21. Where the service user's statement of their postcode is accepted as the organisation’s source, evidence will be required to show that the postcode is regularly checked with the service user on every attendance. There should be audit trail records to show that postcodes are updated appropriately following admissions/attendances, and that there is a mechanism for updating postcodes where independently notified by the service user or GP.

    NB: Birth Episodes do not carry address details for a baby, and should be excluded from the sample group.

Code of Registered GP

22. In many cases there will be enough information in the health records to correctly identify the registered GP. In individual cases where this evidence is not in the case note, the code of Registered GP should be checked against the BSO records, and any discrepancy treated as an inaccuracy. The fact that there may be a time-lag in updates to the BSO records is allowed for in the scoring system.

Process Checks

23. Where the provider can clearly demonstrate that the provider's Board has formally made a policy decision that for named data items the computer is the primary source and that no appropriate source document is being retained, the following alternative approaches should be taken:

    - Where data items are automatically assigned by the computer the accuracy checker will examine the procedures for maintaining the reference files and verify that the assignment process is operating correctly - using a sample of at least 50 records for each affected data item. The accuracy of the data input to the algorithm should also be evaluated.

    - Where data is collected directly onto the computer, the accuracy checker will check the processes for the collection and input of the data item. The reviewer will also check that the processes and procedures are complied with routinely. Again, a sample of at least 50 'transactions' for each applicable data item should be used (NB: multiple data items may be checked simultaneously).

    - Where the service user completes a questionnaire or other written enquiry (such as for capturing Ethnic Category), which is not normally retained either in the health record or elsewhere, the accuracy checker will check that procedures are in place which ensure the accuracy of the data recorded.

24. Organisations should retain the service user questionnaires for a minimum of two years (as per J38 of Good Management Good Records) for scrutiny and sample checking during this check, and these should be available subsequently for evidence. Again, a sample of at least 50 records for each applicable data item should be used.

25. Full details of data definitions and format specifications can also be found in the NI Data Dictionary.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- data quality is addressed as part of the Information Lifecycle Management Policy. Service user data accuracy audits are incorporated into the organisation's audit plan.

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

- the accuracy of service user data audits cover all key data items (or a locally agreed subset). The results are reported to the Board/senior management, or delegated sub-committee as part of ongoing data quality reviews.

- the data quality policy forms part of the broader IG Policy. Actions are taken to address areas of persistently poor data quality.

Examples of evidence include:

- named individuals' job descriptions;
- written procedures;
- communications with staff;
- audit plan
- report for senior management;
- agendas and minutes evidencing that data quality was discussed;
- 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 - 13-506

Criterion 26

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

INFORMATION

Criterion Description

Organisations must ensure that clinical/care staff from all specialties are involved in validating and using the information derived from the recording of clinical/care activity.

Source

- 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

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

GUIDANCE

Validating Information Derived from the Recording of Clinical/Care Activity

1. While ensuring that data is of sufficient quality (and signing the annual declaration to that effect) is a task for corporate management, staff throughout the organisation need the assurance that the underlying data reflects actual service user experiences.

2. The quality of information will not improve unless clinicians and care professionals are fully committed to the process of making their information good enough for their own use. Successful implementation of the Electronic Care Record is dependent upon clinicians and care professionals engaging in improving the quality and consistency of information held about service users.

Involving Clinical/Care Staff in the Validation of Information

3. Involving clinicians or care professionals in validating data is an area where most organisations could improve. Organisations need to begin engaging clinicians and care professionals if this process is not already underway. The approach will vary according to each local organisation's corporate approach to clinical/care engagement and strategy development.

4. What is important is that the organisation engages clinicians and care professionals fully in the process by demonstrating the link between improved information quality, clinical/care and organisational performance and service

user care. As more information is shared electronically the link between information recorded and subsequent care pathways will become ever stronger.

5. Organisations also need to set up a process for Board/senior management level approval of the strategy for clinical/care engagement, and for keeping the process under review in response to changes in service user and care activity.

6. Responsibility for monitoring the effectiveness of the process should be in the terms of reference of a steering group (which may be a pre-existing group, for example an information quality group) or in the job description of a senior individual.

HSC Organisations

7. The Royal College of Physicians (RCP) Health Information Unit has produced a number of guidance documents entitled 'Clinicians Guides to Hospital Data' looking at clinicians responsibilities in relation to the recording and validating of hospital activity data. The RCP guidance states that there are a number of processes in place to validate patient administration system (PAS) data (for example organisational data quality review meetings, clinical audits etc) and there are many ways in which clinicians of any seniority can help data quality. Clinicians could:

    - review the health records of any episodes that the clinical coding department may be having difficulty coding;
    - ask the clinical coding department to determine the top three problem diagnoses or procedures that clinical coding staff encounter within a clinician's specialty;
    - review a proportion of coded Finished Clinical Episodes (FCEs) each month and feed back any problems;
    - ensure that the details of all diagnoses and procedures are clear and easy to find in every set of health records;
    - copy and circulate the **RCPs Top Ten Coding Tips** to junior staff. These are basic note-keeping tips which make a huge difference to coders;
    - encourage juniors to undertake clinical audits using hospital activity data which could then be reviewed by senior clinicians at team meetings/departmental review meetings

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- a strategy for involving clinical/care staff in validating information derived from the recording of clinical/care activity has been developed.

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

- the strategy has been implemented, and clinical/care staff members are involved in validating the data they produce.

- the effectiveness of clinical/care staff validating information derived from the recording of clinical/care activity is monitored and any necessary improvements made.

Examples of evidence include:

- named individuals' job descriptions;
- copy of the strategy;
- improvement plan;
- reports;
- 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 - 13-508

Criterion 27

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

INFORMATION

Criterion Description

There is a comprehensive programme of clinical coding training for clinical coding staff involved in entering coded clinical information conforming to national standards

Source

- Great Britain (1998) the Data Protection Act 1998 Principle 4 and 7 The Stationery Office, London http://www.legislation.gov.uk/ukpga/1998/29/contents

- The inquiry into the management of care of children receiving complex heart surgery at the Bristol Royal InfirmaryDepartment of Health Learning from Bristol: the Department of Health's response to the Report of the public inquiry into children's heart surgery at the Bristol Royal Infirmary 1984-1995: executive summary January 2002 http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4002857

- National Health Service Data Quality Review (NHS) Summer 2012 http://www.connectingforhealth.nhs.uk/systemsandservices/data/clinicalcoding/codingstandards/publications/dqr/dqr_smr_2012.pdf

GUIDANCE

Training Programmes for Clinical Coding Staff

1. Regional training in Northern Ireland is provided following the stipulated national guidelines. These state that the Clinical Coding Foundation Course is delivered over a flexible 25 days depending on the pace of the coders attending.

2. Organisations must ensure that all its clinical coders are sufficiently trained to ensure that they maintain the highest standards of clinical coding. The training given should use material that conforms to national standards. Staff should be offered regular refresher training every two years.

3. The training must be delivered by an NHS Classifications Service approved clinical coding trainer in accordance with the trainer requirements framework and license agreement using only materials developed or endorsed by the NHS Classifications Service or developed in accordance with national clinical coding standards.

4. Furthermore the organisation should provide a training and assessment framework which supports its clinical coders in gaining Accredited Clinical Coder (ACC) status by passing the National Clinical Coding Qualification (UK). This is a marker of good practice and, in so doing, the organisation demonstrates due recognition of the professional status of clinical coding.

5. Clinical coders' is a term used here to describe those who code using ICD-10 and/or OPCS-4.

Evidence demonstrating Compliance

For minimal compliance Organisations should evidence that:

- there is a programme of clinical coding foundation course training conforming to national standards for all clinical coding staff entering coded clinical information.

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

- a programme of clinical coding refresher course training every three years for all clinical coding staff entering coded clinical information is in place that conforms to national standards. All clinical coders are supported in gaining Accredited Clinical Coder (ACC) status by passing the National Clinical Coding Qualification (UK).

- clinical coders have attended clinical coding specialty and update training workshops when classification revisions require.

Examples of evidence include:

- foundation course certificates;
- training plan;
- proof of attendance on refresher courses;
- confirmation of trainer status.

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 - 13-510