Department of Health
www.health-ni.gov.uk

# Records Management

# Good Management Good Records

**2017**

## Contents

# Section 1 Foreword

**Foreword**

*Good Management Good Records* (GMGR) has been published by the Department of Health (DoH) and endorsed by the Chief Executives of the DoH Arms Length Bodies as their Disposal Schedule and a guide to the required standards of practice in the management of records for the DoH and those who work within or under contract to Health and Social Care (HSC) and Public Safety i.e.:

- DoH
- HSC Board;
- Public Health Agency (PHA);
- Business Services Organisation (BSO);
- HSC Trusts;
- Patient and Client Council (PCC);
- Regulation and Quality Improvement Authority (RQIA);
- Guardian AD Litem Agency;
- Blood Transfusion Service;
- Northern Ireland Fire and Rescue Service (NIFRS);
- Northern Ireland Social Care Council (NISCC);
- Northern Ireland Practice and Education Council for Nursing and Midwifery (NIPEC);
- Northern Ireland Medical and Dental Training Agency (NIMDTA);
- Independent Contractors (e.g. general practitioners (GPs), dentists, orthodontists, optometrists and community pharmacists etc.); and
- Early Years Services; Establishments and Agencies where public funds are involved.

For the purposes of this document those mentioned above will be referred to as (Organisation/Organisations).

It is based on professional best practice and reflects the current legal requirements. It is not an authoritative statement of the law, neither does it explain nor replace the law and in cases of doubt Organisations should take legal advice. Where legal proceedings have commenced records should be retained and specific legal advice sought.

It is the responsibility of each organisation to implement and adhere to this Retention and Disposal Schedule. Organisations should ensure that, when referring to legislation, they are aware of any amendments to that legislation. Amendments can be accessed on the Legislation.gov.uk database http://www.legislation.gov.uk and, if necessary, be checked with legal advisors.

GMGR provides a key component of information governance arrangements for the DoH, HSC and Public Safety. As standards and practice change over time, especially with the evolving growth of technology, GMGR will be reviewed and updated as necessary.

**Types of Records covered by GMGR**

The guidelines contained in GMGR apply to the DoH, HSC and Public Safety records of all types (including records of HSC patients treated on behalf of the HSC in the private healthcare sector, or receiving social care services contracted for (procured by) HSC bodies).

These may consist of:

- patient health records (electronic or paper based, including those concerning all specialties, and GP medical records);
- client social care records (electronic or paper based );
- records of private patients seen on HSC premises;[1.]
- accident & emergency, birth, and all other registers;
- theatre registers and minor operations (and other related) registers;
- X-ray and imaging reports, output and images;
- administrative records (including, for example, agendas and minutes of meetings, personnel, estates, financial and accounting records, notes associated with complaint-handling);
- records specified in regulations
- audit and accountability records
- information, technology and communication records and
- governance and policy records.

[1] Although technically exempt from the Public Records Act (Northern Ireland) 1923 it would be appropriate for HSC organisations to treat such records as if they were not so exempt.

**Media of Records covered by GMGR**

The guidelines contained in GMGR apply to all DoH, HSC and Public Safety records regardless of the media on which they are held. Examples of such media are:-

- photographs, slides, and other images;
- microform (i.e. microfiche/microfilm);
- multi media devices;
- e-mails;
- computerised records;
- scanned records;
- text messages (both outgoing and incoming responses);
- social media;
- websites.

# Section 2 Introduction

## Introduction

GMGR 2016 replaces the previous version of GMGR (issued in November 2011).

This guidance provides a framework for consistent and effective records management and is based on advice and publications from the Ministry of Justice, Public Record Office of Northern Ireland (PRONI) and also from best practice followed by a wide range of organisations in both the public and private sectors.

The aims of GMGR are to:

- establish a framework for records management in relation to the creation, use, storage, management and secure disposal (destruction or archiving) of all types of DoH, HSC and Public Safety records;
- clarify the legal obligations in relation to records management and information access;
- explain the actions required by Chief Executives and other managers to fulfil these obligations;
- explain the requirement to select records for permanent preservation as directed by PRONI;
- set out the minimum periods for retention of all types of DoH, HSC and Public Safety records, regardless of the media on which they are held; and
- indicate where further information on records management may be found.

GMGR is a legal document, approved by the Northern Ireland Assembly, authorising the disposal of records that fall into one of the disposal classes listed in the schedule. Disposal classes are categories of records derived from business functions and activities.

**General Context**

All DoH, HSC and Public Safety records are public records under the terms of the Public Records Act (Northern Ireland) 1923 (PRA 1923). The PRA 1923 established PRONI as the place of deposit for public records, created the roles of Keeper and Deputy Keeper of the records as well as defining NI public records. The PRA 1923 sets out the broad responsibilities for everyone who works with such records. Organisations have a statutory duty to make arrangements for the safe keeping and eventual secure disposal of their records. PRONI can assist and provide advice on how to manage all types of records.

The PRA 1923 made PRONI responsible for the records of any Court, Government Department, Authority or Office in Northern Ireland over which the Parliament of Northern Ireland (NI) has the power to legislate. It is therefore a statutory requirement for the HSC and Public Safety to implement records management as set out in the PRA 1923 and in the Disposal of Documents (NI) Order (1925). PRONI has an overarching responsibility within the public sector in NI to ensure that records are managed in accordance with agreed policies and procedures. In particular:

- PRONI is concerned with identifying any deficiencies in the way records are organised and maintained and in records management procedures as a whole.
- PRONI must be involved in:
    - updating and quality assurance of all Disposal Schedules;
    - the sampling of Particular Instance Papers (case files);
    - ensuring the proper use of microfilm and other non-paper based storage media e.g. records held electronically;
- the assessment of records for historical/research purposes;
- the storage of records identified for permanent preservation and which are no longer required by Organisations for administrative/business purposes.

The Permanent Secretary, Departmental Information Manager (DIM), Chief Executives and senior managers are personally accountable for records management within their Organisation and have a duty to make arrangements for the safe keeping and eventual disposal of those records under the overall supervision of the Deputy Keeper of Public Records at PRONI. Organisations are also required to take positive ownership of, and responsibility for, the records legacy of predecessor Organisations and/or obsolete services.

Robust records management procedures are required to meet the requirements set out under the Data Protection Act 1998 (DPA 1998), the Freedom of Information Act 2000 (FOI Act 2000) and the Environmental Information Regulations 2004 (EIR 2004).

Records are a valuable resource because of the information they contain. High-quality information underpins the delivery of high-quality evidence-based health and social care, and many other key service deliverables. Information has most value when it is accurate, up to date and accessible when it is needed. An effective records management system ensures that information is properly managed and is available whenever and wherever there is a justified need for that information to:

- support patient / client care and continuity of care;
- support service provision;
- support day-to-day business which underpins the delivery of care;
- support evidence-based clinical practice;
- support sound administrative and managerial decision making, as part of the knowledge base for DoH, HSC and Public Safety services;
- meet legal requirements, including requests from the public under subject access provisions of the DPA 1998, FOI Act 2000 or EIR 2004;
- assist clinical/professional and other types of audits;
- support improvements in clinical/professional and service effectiveness through research and also to support archival functions by taking account of the historical importance of material and the needs of future research; or
- support choice and control of patients and clients over treatment and services.

The increasing shift towards electronic records will transform the way health and social care information is managed. In the mixed economy of paper and electronic records it is essential that they are managed consistently to ensure that a complete record is available at the point of need.

GMGR identifies the specific actions, managerial responsibilities and minimum retention periods for the effective management of all types of DoH, HSC (i.e. both corporate and individual health and social care records) and Public Safety records, regardless of whether they are paper or electronic, from creation to disposal.

**Monitoring Records Management Performance**

A number of bodies have oversight of DoH, HSC and Public Safety performance in respect of records management. The Regulation and Quality Improvement Authority monitors a core governance standard relating to broad records management as part of its annual assessment of performance. The Audit Commission regularly conducts studies into records management and related data quality issues. The DoH collects performance details as part of the annual Controls Assurance Standards.

Other bodies likely to comment on records management performance include the Northern Ireland Ombudsman when investigating a complaint, and the Information Commissioner when investigating alleged breaches of the DPA 1998 or the FOI Act 2000 or in promoting the Lord Chancellor's Code of Practice on Records Management under section 46 of the FOI Act 2000 and PRONI.

## Legal and Professional Obligations

The principle legislation governing the management of records is the Public Records Act (NI) 1923. All individuals who work for an Organisation are responsible for any records which they create or use in the performance of their duties. Such records are public records and may be subject to both legal and professional requirements.

A key statutory requirement for compliance with records management in relation to records containing personal data lie within the principles of the DPA 1998. The DPA 1998 regulates the processing of all personal data, held both manually and on computer.

Personal data is defined as data relating to a living individual that enables him/her to be identified either from that data alone or from that data in conjunction with other information in the data controller's possession.

## Disclosure of Information and Transfer of Records

The Freedom of Information Act (FOIA) 2000 lays down requirements for public bodies (including the HSC) to keep and make information available on request. They are additional to other access rights, such as access to personal information under the Data Protection Act 1998, access to environmental information under the EIR 2004, and access to health records under the **Access to Health Records (Northern Ireland) Order 1993**.

There is also a range of guidance documents (for example the Information Commissioner's Use and Disclosure of Health Information) that interpret statutory requirements.

Consideration should also be given to the application of the Data Protection (Subject Access Modification) (Health) Order 2000 which exempts disclosure of information which may be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person.

It is particularly important under Freedom of Information legislation that the disposal of records – which is defined as the point in their lifecycle when they are either transferred to PRONI or destroyed – is undertaken in accordance with clearly established policies which have been formally adopted by the Organisation and which are enforced by properly trained and authorised staff.

The mechanisms for transferring records from one Organisation to another should also be tailored to the sensitivity of the material contained within the records and the media on which they are held. Information Security staff should be able to advise on appropriate safeguards.

The protocol for the hospital transfer of patients and their records http://www.gain-ni.org/images/Uploads/Guidelines/protocol.pdf should be adhered to when hospital patient records are being transferred. The regional discharge and patient transfer protocol for patients with clostridium difficile infection should be adhered to as appropriate. For standards of the handover and discharge record clinical content see https://www.rcplondon.ac.uk/projects/outputs/generic-medical-record-keeping-standards

https://www.rcoa.ac.uk/sites/default/files/FPM-clinicians-guide1.pdf

For GP records see Good Practice Guidelines for General Practice Electronic Patient Records (version 3.1), for guidance on the transfer of electronic patient records from one GP practice to another.

Guidance documents and additional materials on Freedom of information and Data Protection can be found on the Information Commissioner's website: https://ico.org.uk/

**Protecting the Confidentiality of Service User Information**

**Code of Practice on Protecting the Confidentiality of Service User Information**

A revised Code of Practice on Protecting the Confidentiality of Service User Information was issued in January 2012. The revised Code is aimed at supporting staff in making good decisions about the protection, use and disclosure of service user information. The Code of Practice should be the reference point for all staff.

**The Protocol**

The DHSSPS and HSC Protocol for sharing service user information for secondary purposes was developed to support and reinforce the principles and guidelines in the Code. It provides a framework for sharing personal information about service users, between partner organisations in Northern Ireland, which is in line with the Code of Practice.

**Data Access Agreements**

When sharing HSC data for non direct care (secondary purposes), requesting organisations are required to provide assurances that they comply with the Data Protection Act (1998) and that they have relevant DPA Policies and Procedures in place which their staff are aware of. A Data Access Agreement must be completed by any organisation wishing to access HSC Trust data. It must be considered for approval and signed by the supplier organisation's Personal Data Guardian.

# Section 3 Records Management

The ISO standard, ISO 15489-1:2016 Information and documentation - Records management [2] defines the concepts and principles for the creation, capture and management of records.

**What is a record?**

A record is information that has been received, created or maintained by an individual or an Organisation as evidence of a business activity, patient/client care, treatment given, treatment planned and can be in any format – paper, electronic, digital and/or voice.

In the context of GMGR a record is anything which contains information (in any media) which has been created or gathered as a result of *any* aspect of the work of employees or those providing a service– including consultants, General Practitioners, Dentists , Opticians, Pharmacists, agency, or casual staff and all contracted services.

DoH, HSC and Public Safety records are public records as defined in the PRA 1923.

**Why do you need to keep records**

Records enable Organisations to:

- conduct business in an orderly, efficient and accountable manner;
- deliver care and services in a consistent and equitable manner;
- support and document policy formation and managerial decision-making;
- provide consistency, continuity and productivity in management and administration;
- facilitate the effective performance of activities throughout the DoH, HSC and Public Safety;
- provide continuity in the provision of services, care, or treatment;
- provide continuity in the event of a disaster;
- meet legislative and regulatory requirements including archival, audit and oversight activities;
- provide protection and support in litigation including the management of risks associated with the existence of or lack of evidence of DoH, HSC and Public Safety activity;
- protect the interests of the DoH, HSC and Public Safety and the rights of employees, patients, clients, and present and future stakeholders;
- support and document current and future research, inform future service and document activities, developments and achievements, as well as historical research;
- establish and provide evidence of business, personal and cultural identity; and

[2] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62542

- maintain the corporate, personal or collective memory.

**What is Records Management**

Records management is:

- the systematic and consistent control of all records, regardless of the media on which they are held, throughout their lifecycle. It includes setting up the infrastructure or system into which the records are created, received or added as well as the process of record creation itself.
- organising the records so that related records are grouped together, usually according to a file plan or classification scheme. (Managing groups of related records is more efficient than managing many individual records.)
- the retention and disposal actions such as destruction or transfer to PRONI at the appropriate time and procedures for documenting those actions.

Organisations must know what records they have in order to manage them. Control of the records depends on a range of carefully developed procedures applied to them before their creation through to their disposal.

There are five vital elements of records management:

- meeting business and patient/client needs;
- public records legislation;
- managing records as a valuable and expensive asset;
- defensible disposition[3] accountability for practice and service provision; and
- accountability and quality of information and services.

[3] the process by which corporate content is systematically deleted with an audit trail that will be defensible in court

## Management and Organisational Responsibility

### Records Management

Organisations should have in place organisational arrangements that support records management. The records management function should be recognised as a specific corporate responsibility within every Organisation. 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 disposal. It should have clearly defined responsibilities and objectives, and adequate resources to achieve them and should include records managed on behalf of the authority by an external body such as a contractor.

Records and information management should be included in the corporate risk management framework. Information and records are a corporate asset, the loss of which could cause disruption to the business of the Organisation. The level of risk will vary according to the strategic and operational value of the asset to the Organisation and risk management should reflect the probable extent of disruption and resulting damage.

Organisations should have a governance framework that includes defined roles and lines of responsibility. This should include allocation of lead responsibility for the records and information management function to a designated member of staff at sufficiently senior level to act as a records management champion, for example a board member, and allocation of operational responsibility to a member of staff with the necessary knowledge and skills. In smaller organisations it may be more practicable to combine these roles. Ideally the same people will be responsible also for compliance with other information legislation, for example the Data Protection Act 1998 and the Re-use of Public Sector Information Regulations 2005, or will work closely with those people. These roles should be formally acknowledged and made widely known throughout the Organisation.

The organisation should have in place clear instructions covering the creation, maintenance and management of records which apply to staff at all levels of the Organisation. In larger organisations the responsibilities of managers, and in particular heads of business units, could be differentiated from the responsibilities of other staff by making it clear that managers are responsible for ensuring that adequate records are kept of the activities for which they are accountable;

Organisations should identify information and business systems that hold records and provide the resources needed to maintain and protect the integrity of those systems and the information they contain.

Organisations must consider records management issues when planning or implementing ICT systems, when extending staff access to new technologies and during re-structuring or major changes to the Organisation.

All staff must be appropriately trained so that they can carry out their designated duties and responsibilities. Induction and other training should ensure that all staff are aware of the authority's records management policies, standards, procedures and guidelines and understand their personal responsibilities. This should be extended to temporary staff, contractors and consultants who are undertaking work that it has been decided should be documented in the authority's records. This should include training for staff in the use of electronic records

systems. Training should be provided through both generic and specific training programmes, complemented by organisational policies and procedures and guidance.

If the Organisation is large enough to employ staff whose work is primarily about records and information management, they should be given opportunities for professional development.

**Information Assurance Roles**

The DoH, HSC and Public Safety Organisations have established Information Governance Roles within their organisations.

**Senior Information Risk Owner**

The Senior Information Risk Owner (SIRO) is an Executive Director or Senior Management Board Member. The **SIRO** is the focus for the management of information risk at Board level and should:

- lead and foster a culture that values, protects and uses information for the public good;
- own the overall information risk policy and risk assessment process, test its outcome and ensure it is used;
- advise the accounting officer on the information risk aspects of his governance statement.

**Information Asset Owner**

Information Asset Owners are senior individuals, directly accountable to the SIRO, who are required to provide assurance that information risk is being managed effectively for their assigned information assets. Their role is to understand what information is held, what is added and what is removed, how information is moved, advise on the appropriate classification and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good, and provide written input to the SIRO annually on the security and use of their asset.

**Individual Responsibility**

The PRA 1923 makes all employees responsible for any records that they create or use in the course of their duties. Staff are responsible for maintaining their records in accordance with their Organisation's Records Management Policy. In particular

1. following the procedures endorsed by senior management; and
2. only destroying records in accordance with the Organisation's Disposal Schedule and procedures.

**Information and Records Management Policy**

Each Organisation should have in place an Information and Records Management Policy defining how it manages all of its records, including electronic records. The policy should be endorsed by the Organisation's Board and made available to all staff at all levels of the Organisation, both on induction and at regular training.

# Section 4 Records Management Processes

**Records Management Processes**

Implementing and maintaining effective records management depends on the knowledge of what records are held, where they are stored, who manages them, in what format(s) they are made accessible, and their relationship to organisational functions (for example finance, estates, IT, healthcare or social care provision). An information survey or record audit is essential to meeting this requirement.

There should also be audits of the content of clinical records. The Academy of Royal Colleges (AoMRC) provides generic medial record keeping standards (hosted by the Royal College of Physicians). Further information about professional standards for records can be obtained from the appropriate professional body.

- The General Medical Council
  http://www.gmc-uk.org/guidance/index.asp

- The British Medical Association (BMA)
  http://bma.org.uk/practical-support-at-work/ethics/confidentiality-and-health-records

- Royal College of Physicians
  https://www.rcplondon.ac.uk/resources/generic-medical-record-keeping-standards

- Royal College of General Practitioners (with DH and the BMA))
  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/215680/dh_125350.pdf

- Royal College of Nursing
  http://www.rcn.org.uk/get-help/rcn-advice/record-keeping

- Nursing and Midwifery Council
  https://www.nmc.org.uk/

- Royal College of Pathologists
  https://www.rcpath.org/resourceLibrary/the-retention-and-storage-of-pathological-records-and-specimens--5th-edition-.html

- Health and Care Professions Council
  http://www.hcpc-uk.org/

## Record Creation

It is the responsibility of each Organisation to ensure that all records are complete, reliable, authentic and available regardless of the media on which the records are kept. In addition, Organisations must be satisfied that all records are kept in an accessible format.

Organisations should have in place a process for documenting its records management activities. Records should accurately reflect communications, decisions and actions taken.

Records should be arranged in a record-keeping system that will enable the Organisation to ensure the quick and easy retrieval of information.

## Registration of Records

Registration is a system which allocates a unique identifier (numerical and alphabetical prefix) to each record and which annotates that sequentially in a 'register' or index. It provides evidence that a record has been created or captured and facilitates retrieval.

Paper and electronic record keeping systems should contain descriptive and technical documentation to enable the system to be operated efficiently and the records held in the system to be understood.

The record keeping system, whether paper or electronic, should include a documented set of rules for classification, titling, indexing and, if appropriate, the protective marking of records. These should be easily understood to enable the efficient retrieval of information when it is needed and to maintain security and confidentiality.

The Northern Ireland Records Management Standard (NIRMS) - Filing Systems, gives guidance on the types of paper based systems.

## Digital Continuity

Digital continuity is the ability to use electronically created records for as long as they are needed. In some cases this may mean having to manage electronic records which need to be permanently preserved.

Organisations who choose to install electronic record creation systems should take into account the need to manage the records created for the entirety of their lifecycles.

How Organisations use, and maintain, records created within electronic systems will largely depend on the nature of the Organisation and the information itself. In some cases full functionality will be required for the records for the entirety of their lifecycles, whereas for others the ability to read the records may be enough.

Digital information must be stored in such a way that throughout the lifecycle it can be recovered in an accessible format. The electronic filing structure must capture all metadata needed to identify, access and retrieve the electronic record so that it is possible to establish the

context of the records, who created it, during which business process, and how the record is related to the other records;

Appropriate references linking the electronic file to the paper file must be used in order that retention criteria can be applied consistently

The authenticity and integrity of a record must be maintained.

**Electronic Document Records Management System (EDRMS)**

An electronic document becomes an electronic record if it provides evidence of a business transaction and is saved and finalised within an EDRMS. An EDRMS provides a corporate filing structure and facilitates the automatic disposal and retention of records.

**File Plans / Classification Schemes**

A File Plan is an essential component of a records management programme developed in line with BS ISO 15489-1:2016, the International Standard on Information and Documentation - Records Management. File plans and their associated metadata are vital to the successful implementation of any Electronic Document Records Management system (EDRMS).

A File Plan may also be described as a Classification Scheme for arranging records based on the functions and activities of the Organisation. Such a scheme or file plan facilitates the creation and retrieval of electronic records, particularly where large amounts of data are involved.

**Scanning**

For reasons such as business efficiency or to address problems with storage space, Organisations may consider the option of scanning into electronic format records which exist in paper format. Where this is proposed, the factors to be taken into account include:

- the need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008-1:2014)[3];
- the need to consult PRONI in advance with regard to records which may have archival value, as the value may include the format in which it was created; and
- the costs of the initial and then any later media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept

The decision on whether or not the original paper documentation can be destroyed once it has been scanned is a decision that each Organisation as a Data Controller must make. It cannot be assumed that because an EDRMS system is in place, all the documents within the system

are necessarily admissible as evidence before a court. One of the key important steps is an audit of the system using the British Standard BIP 0009:2015, Evidential Weight and Legal Admissibility of Electronic Information Compliance Workbook. EDRMS's are very configurable, but it is extremely important that they are configured in a way that complies with the criteria in the standard.

The legal admissibility of scanned records, as with any digital information, is determined by how it can be shown that it is an authentic record. There is no absolute guarantee that any digital record will be accepted in a court of law, as it is often down to individual judges whether they will accept it as evidence. The standard, 'BS ISO 10007:2003 Electronic Information Management - Ensuring the authenticity and integrity of electronic information', outlines the method of ensuring that electronic information remains authentic[4]. The standard deals with both 'born digital' and scanned records.

Whilst compliance with the relevant standards does not guarantee legal admissibility it enables organisations to demonstrate that they are following best practice.

[3]http://shop.bsigroup.com/ProductDetail/?pid=000000000030296631

[4] *BS 10008:2014 has now been published.* A new version of BS 10008 for an electronic information management system http://www.bsigroup.com/en-GB/bs-10008-electronic-information-management/

## Microfilming Records

Microfilm records can be certified as providing legally admissible archival documents but specific standards for microfilming of records need to be met. The National Preservation Office (allied to the British Library) has produced standards (Guide to Preservation Microfilming 2000) for preservation microfilming which are acceptable to archive institutions throughout the UK.

## Email as a Record

It is hard to imagine a more important record than email, which is why it deserves a special mention in this Code[5]. Email has the benefit of fixing information in time and assigning the action to an individual - which are two of the most important characteristics of an authentic record.

The great problem with email is that it is rarely saved in the business context, which is the third characteristic to achieve an authentic record. The correct place to store email is in the record keeping system according to the business classification scheme or file plan activity to which it relates. Where email is declared as a record, the entire email must be kept including attachments so the record remains integral.

## System Back Ups

System Back Ups, some of which would be clinical information, should be retained for the minimal period consistent with business continuity and patient safety considerations. These are not records rather a process in which the state, files and data of a system is duplicated to be used as a backup or data substitute when the primary system data is corrupted, deleted or lost.

## Social Media

Where social media is used as a means of communicating information for business purposes, or a means of interacting with clients, it may be a record that needs to be kept. Where this is the case information must be retained within the record keeping system. This may not necessarily mean that the social media must be captured but rather the information of the activity through transcription or periodic storage.

## Website as a Business Record

As citizens interact with their public services, it is the internet and websites in particular that provide information - just as posters, publications and leaflets once did exclusively.

[5] See TNA Managing emails
http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/managing-email/

Websites form part of the record keeping system and must be preserved. It is also important to know what material was present on the website as this material is considered to have been published. For this reason the frequency of capture must be adequate.

It may be possible to arrange regular crawls of the site with PRONI, but given the complexity of sites as digital objects, it may be necessary to use other methods of capture to ensure that this creates a formal record. PRONI intend to crawl the NI Government Department websites twice a year (June and November) and their website has some information on the project:

http://www.proni.gov.uk/index/search_the_archives/proniwebarchive/web-archive-faqs.htm

You can find a copy of the crawls that have been completed to date via PRONIs web archive: http://www.proni.gov.uk/index/search_the_archives/proniwebarchive.htm

**Cloud Based Records**

Use of cloud based solutions are increasingly being considered as an alternative to managing large networks and infrastructure. Before any cloud based solution is implemented there are a number of records considerations that must be addressed[6].[7]

For example:

All HSC and Public Safety organisations must ensure that ICT & information security clauses, particularly with regards to the Data Protection Act 1998, are built into all formal service contracts.

Where data is being hosted external to the HSC and Public Safety network, information-based risk assessments are required to be carried out, which consider (as a minimum) legislation and implications with regards to:

- hosting outside the EU (if applicable)
- business continuity planning
- physical & logical access management
- audit logging & access to logs/reports
- termination of contract
- disposal of information in line with GMGR

Specific consideration should be given to the termination of the contract. The service provider or solution may change and it will be necessary to migrate all of the records onto another solution. This may be technically challenging. As part of the contract, it is also important to ensure that the original provider securely deletes your information/data once it is transferred to the new service or when the service is decommissioned.

The Information Commissioners Office Guidance on the use of cloud computing advises how the security requirements of the DPA apply to personal data processed in the cloud.

[6] TNA Guidance on Cloud Storage and Digital Preservation
http://www.nationalarchives.gov.uk/documents/CloudStorage-Guidance_March-2015.pdf

[7] **Good Practice Guide No. 6**
**Outsourcing & Offshoring: Managing the Security Risks**
Issue No: 2.1
September 2010 http://www.nationalarchives.gov.uk/documents/CloudStorage-Guidance_March-2015.pdf

**Retention and Disposal Arrangements**

The retention periods for DoH, HSC and Public Safety records are provided in Part 2 of GMGR and apply to electronic and paper records. It has been agreed with PRONI which records they want to permanently preserve and which are to be appraised, to give Organisations and PRONI the chance to determine their evidential or historical importance at a later date. As medical technologies and care advances are made PRONI wish to preserve records of individually significant cases. These records should be identified at the earliest point and marked in some distinctive way to ensure they are transferred to PRONI once they have reached 20 years old (as calculated from the date of the last paper).

The classes of records to be appraised will involve a consultation between PRONI, and Organisation medical and records management professionals. All Organisations are required to have internal procedures to ensure records listed for permanent preservation are transferred to PRONI, records listed for destruction are destroyed and records requiring appraisal are appraised.

Records identified by medical and/or records management professionals for PRONI appraisal should be based on their value of potential significance e.g. medical, evidential, or historical. This identification exercise should be completed at the point of record closure before the commencement of the retention period. When a record identified for appraisal reaches the end of its retention period and there is no longer a business need for retention, PRONI should be contacted. Records management staff should provide PRONI with details of the files requiring appraisal. If feasible, this would in the form of an inventory. This inventory should include details such as titles of records, dates, a brief description of the contents, volume, location and any other information that may be helpful. PRONI may require additional input from medical and/or records management professionals prior to or during the appraisal process. This is likely to involve professionals who have knowledge of the content of the records e.g. medical staff who have an understanding of the medical terms used and who may be able to assist PRONI during the appraisal process. Any additional input required will be discussed when the inventory has been received by PRONI".

It is particularly important under Freedom of Information legislation that the disposal of records – which is defined as the point in their lifecycle when they are either transferred to PRONI or destroyed – is undertaken in accordance with clearly established policies which have been formally adopted by the Organisation and which are enforced by properly trained and authorised staff.

The principles governing the closure and subsequent retention of electronic records are identical to those for paper records

If a file is to be deleted, then it is the data controller's responsibility to ensure it is also deleted from any back-up systems. Information in a deleted file or in a back-up, whether a server, disc or tape, may be regarded as being held by a public authority for the purposes of the FOIA depending on the particular circumstances of the individual case.

**Transfer of Records to PRONI**

Records selected by PRONI for permanent preservation and no longer in use by the organisation should be transferred as soon as possible to PRONI. The 1923 PRA established the normal point of transfer as 20 years.

**Transfer of Paper Records**

Public Bodies in Northern Ireland should follow the guidance "Transfer of Official Paper Records to the Public Record Office of Northern Ireland"
https://www.nidirect.gov.uk/publications/guidance-transfer-official-paper-records

**Transfer of Electronic Records to PRONI**

On 31st March 2015, PRONI completed a project to develop a trusted digital repository capable of 'ingesting' digital records. The primary aim of this system is to store, preserve and provide access where possible to digital records.

Electronic records in RecordsNI (the NI Civil Service Electronic Document and Records Management System) identified for permanent preservation in this Disposal Schedule, should be transferred in accordance with PRONI's *Digital Repository - Submission Guidance (RecordsNI).* This document provides guidance for Records Managers with responsibility for transferring electronic records from RecordsNI to PRONI and is available from your Departmental Information Manager.

Guidance for Public Sector Bodies transferring electronic records to PRONI from systems other than RecordsNI is available on the PRONI website .

Those records not required by PRONI for permanent preservation should be destroyed as soon as their business need comes to an end.

While the Disposal Schedule in Part 2 applies to both electronic and paper records, the creation of electronic disposal schedules within an Electronic Document Records Management System may require a separate project to ensure their operational viability.

Organisations which have already implemented electronic record keeping systems should contact PRONI for the advice and guidance required to plan for the transfer of records.

**Disposal Schedules**

A disposal Schedule is the key document in a records management system which:

- enables the Organisation to meet legislative requirements;
- outlines the types of records held within an Organisation;
- outlines the associated legislative/policy guidance framework;
- identifies the minimum period for which records should be retained; and
- outlines the action required when the minimum retention period has been reached.

This document defines the minimum length of time specific types of records have to be retained before being appraised, destroyed or transferred to PRONI. Records fall into four main categories of action:

- Records to be destroyed after an agreed period (e.g. a file containing receipts for registered and recorded delivery mail is retained for 2 years following the financial year to which they relate and then destroyed). Files with specified destruction dates should be destroyed securely;
- Records selected for permanent preservation by PRONI;
- Records to be appraised; and
- Records which are required to be kept permanently in the organisation i.e. benefactions, where the benefactory endowment trust fund/capital remains permanent.

There are 4 options when the minimum retention period has been reached:-

- PRONI Appraisal
- Retain Permanently within the organisation
- Permanent Preservation
- Destroy

Guidance on these options is covered within the Northern Ireland Records Management Standard, NIRMS.

**Record Disposal**

Most Organisations' records, even administrative ones, contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage of the lifecycle of the record, including destruction, and that the method used to destroy such records is fully effective and ensures their complete illegibility.

It is the responsibility of the Organisation to ensure that the methods used throughout the destruction process provide adequate safeguards against the accidental loss or disclosure of the contents of the records. Contractors, if used, should be required to sign confidentiality undertakings and to produce written certification as proof of destruction. Organisations should monitor performance against the contract. A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the Records Manager, so that the organisation is aware of those records that have been destroyed and are therefore no longer available. Disposal schedules would constitute the basis of such a record.

If a record due for destruction is known to be the subject of a request for information, or potential legal action, destruction should be delayed until disclosure has taken place, or if the authority has decided not to disclose the information, until the complaint and appeal provisions of the Freedom of Information Act have been exhausted or the legal process completed, as deletion may be an offence within the DPA 1988.

# Section 5 Special Category Records

## Special Category Records

Some classes of information may need special arrangements to be made for their registration or appraisal. Such records may be termed as 'special category records' and may be treated as such for a variety of reasons including the:

- importance of the record;
- confidentiality of the record;
- use to which the record is put.

A record is not distinguished as a special category record simply because of its actual nature, rather it is distinguished because for official purposes it needs to be treated differently from the other records.

The Records Management Officer should be advised of the existence of any special category records and arrangements must be put in place to ensure that they are subject to the normal review procedure, or that a special appraisal is agreed with PRONI. Special category records held on paper should not be held on unregistered files.

## Photographs, Sound Recordings, Cinematograph Files, Videocassette Recordings and Machine Readable Records

Photographs, sound recordings, cinematograph files, videocassette recordings and machine-readable records are public records and should be included in any Disposal Schedule. The Public Records Act (NI) 1923 is intended to preserve important information in whatever forms it is stored. Given the nature of these items, special storage arrangements might be required. Arrangements for storage, appraisal and/or permanent preservation should be made with the Records Management Officer at the earliest possible opportunity, preferably before creation.

Further guidance about audiovisual records may be obtained from the National Archives (London) website:

http://www.archives.gov/records-mgmt/publications/managing-audiovisual-records.html

**Papers of Temporary Commissions, Committees and Review Bodies (including Non-Departmental Public Bodies)**

Papers of temporary commissions, committees and review bodies (including those relating to non-departmental public bodies) are always exempt from normal review periods. The Retention and Disposal of such records should be considered at the outset and the Public Record Office engaged to ensure that they are aware of the records and the format in which they are being created.

They should be dealt with immediately after the work of the commission, Committee or Body has finished. The Secretary of the body should contact the Records Management Officer, the DoH Departmental Information Manager and PRONI when the body is drawing to a close. Arrangements can then be made for the retention and disposal of the records.

It will also be necessary for the body to complete PR14 forms before the records transfer to PRONI.

**Statute-Barred Records**

Many statutes e.g. the Food and Drugs Act (NI) 1958 require the general public or sections of it to furnish Government with personal or commercial information. The confidentiality of this information is guaranteed by the inclusion in the statute of a section barring those involved in collecting or collating of the information from divulging it, except where official duties so require. Records in a statute –barred class should be clearly identified in any disposal schedule and cannot under current legislation be released to the public at any time and are therefore not subject to the normal appraisal procedures.

The Rehabilitation of Offenders (NI) Order 1978 precludes the release of information about 'a living identifiable individual' who has been charged with or convicted of an offence resulting in a fine or in a sentence of imprisonment or corrective training for a term of up to 30 months. Depending on the age of the person at the time and the term of sentence, a person is considered to have been rehabilitated after a specified number of years and thereafter no details of 'spent convictions' may be made public. In accordance with a guideline set down by the Northern Ireland Office (now the Department of Justice) such material remains closed until the person would be deemed to have reached the age of at least 95 years.

**Inquiries - Under Legislation**

The Inquiries Act 2005 (c.12) provides as follows:

A Minister may cause an inquiry to be held under this Act in relation to a case where it appears to him that -

(a) particular events have caused, or are capable of causing, public concern, or

(b) there is public concern that particular events may have occurred.

The Inquiry papers should be dealt with immediately after the Inquiry is completed. It is not necessary to wait until the papers reach the normal age for review. The secretary to the Inquiry should inform both the DoH DIM and PRONI when the Inquiry is thought to be drawing to a close. Arrangements can then be made for the proper retention and disposal of records.

Retained records will be transferred to PRONI directly from the Inquiry secretary. These records will require PR14s to be completed.

**Departmental Inquiries - Administrative**

An Internal Departmental Inquiry may be initiated by a Minister or Permanent Secretary, with no statutory basis. The records should be reviewed once the Inquiry is complete. The final action will be determined by PRONI on appraisal.

**Further Guidance**

Further information on special category records may be obtained on the PRONI website (https://www.nidirect.gov.uk/publications/northern-ireland-records-management-standard-nirms-special-category-records).

# Annex A

## Annex A – Contacts, Resources, Standards, and Guidelines to Support Improvement

### Contacts

**Information and Records Management Society**

**Web:** www.irms.org.uk

**Information Commissioner**

**Web:** https://ico.org.uk/about-the-ico/who-we-are/northern-ireland-office/

https://ico.org.uk/

**Information Management Branch -** Department of Health

**Web:** https://www.health-ni.gov.uk/

**Email:** gmgr@health-ni.gov.uk

**The Privacy Advisory Committee in Northern Ireland**

**Web:** http://www.privacyadvisorycommittee.hscni.net/

**Institute of Health Record and Information Management (IHRIM)**

**Web:** http://www.ihrim.org/

**National Preservation Office** - The British Library
**Web:** www.bl.uk

**International Council on Archives**

**Web:** http://www.ica.org/

**The National Archives**

**Web:** http://www.nationalarchives.gov.uk/

**The Public Record Office of Northern Ireland**

**Web:** https://www.nidirect.gov.uk/proni

## Resources, Standards and Guidelines

Information Commissioner: Use and Disclosure of Health Data
https://www.igt.hscic.gov.uk/Knowledgebase/Kb/Information%20Commissioner/IC_Use%20and%20disclosure%20of%20health%20data.pdf

Information Commissioner: CCTV Code of Practice
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Information Commissioner: Data Sharing Code of Practice https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

The Information Management Controls Assurance Standard
https://www.health-ni.gov.uk/publications/controls-assurance-standards

Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 First published in November 2002, the code was revised and re-issued in July 2009
http://www.nationalarchives.gov.uk/documents/information-management/foi-section-46-code-of-practice.pdf

The National Archives Information Management Guidance
http://www.nationalarchives.gov.uk/recordsmanagement/selection/acquisition.htm#5
http://www.nationalarchives.gov.uk/recordsmanagement/advice/standards.htm
http://www.nationalarchives.gov.uk/documents/information-management/sched_personnel.pdf

International record keeping standards.
BS ISO 15489-1:2016 – Information and documentation – Records management.
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62542

(BIP 0008: 2004 – Copyright BSI). British Standards Institution. Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically
http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030104568
ISO 19005 – 1:2005 Document Management
http://www.iso.org/iso/catalogue_detail?csnumber=38920

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

e-Government Technical Standards
http://standards.data.gov.uk/

**Records Management Code of Practice for Health and Social Care 2016**
http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf

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

Royal College of Nursing
http://www.rcn.org.uk/

Standardisation Committee for Care Information
www.hscic.gov.uk/isce

The General Medical Council
http://www.gmc-uk.org/guidance/index.asp

The British Medical Association (BMA)
http://bma.org.uk/practical-support-at-work/ethics/confidentiality-and-health-records
https://www.bma.org.uk/membership?utm_source=bing&utm_medium=cpc&utm_campaign=BMA

Health and Care Professions Council
http://www.hcpc-uk.org/

Good Practice Guidelines for General Practice Electronic Patient Records (version 4) - prepared by the Joint Computing Group of the General Practitioners Committee and the Royal College of General Practitioners, sponsored by the Department of Health. It can be found at:

http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_125310

The Royal College of Pathologists: https://www.rcpath.org/resourceLibrary/the-retention-and-storage-of-pathological-records-and-specimens--5th-edition-.html

(BASHH) Guidance on the Retention and Disposal of Hospital Notes: http://www.bashh.org/documents/1062/1062.pdf

The Medical Protection Society has published guidance, Keeping Medical Records – A Complete Guide for Consultants. It is available on their website, see: www.medicalprotection.org

Confidentiality: DoH Code of Practice on Protecting the Confidentiality of Service User Information (PDF 249KB) https://www.health-ni.gov.uk/publications/dhssps-code-practice-protecting-confidentiality-service-user-information

Medical Research Council: *http://www.mrc.ac.uk/news/publications/human-tissue-and-biological-samples-for-use-in-research/*.

Medicines and Healthcare Products Regulatory Agency. *Management and Use of Point of Care Test Devices.* MDA DB 2002(03), 2002
www.mhra.gov.uk

UK Newborn Screening Programme Centre - *Code of Practice for the Retention and Storage of Residual Newborn Blood Spots, 2005*.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415981/Code_of_Practice_for_the_Retention_and_Storage_of_Residual_Blood_Spots.pdf

Guidance on the Microbiological Safety of Human Organs, Tissues and Cells used in Transplantation August 2000. This guidance updates and replaces the 'Guidance on the Microbiological Safety of Human Tissues and Organs used in Transplantation' issued in 1996. https://www.gov.uk/government/publications/guidance-on-the-microbiological-safety-of-human-organs-tissues-and-cells-used-in-transplantation

The Minimum Standards for Dental Care and Treatment https://www.health-ni.gov.uk/articles/chief-dental-officer-highlights-mouth-cancer-action-month

Legal and Professional Obligations

There are a range of legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed. The following is a list of the key legal and professional obligations covering personal and other information:

- The Access to Health Records (Northern Ireland) Order 1993
- The Access to Personal Files and Medical Reports (Northern Ireland) Order 1991
- Administrative Law
- The Adoption Agencies Regulations (Northern Ireland) 1989
- The Blood Safety and Quality Regulations 2005 (as amended)
- The Census (Confidentiality) (Northern Ireland) Order 1991
- The Civil Evidence (Northern Ireland) Order 1997
- The Common Law Duty of Confidentiality
  – Confidentiality: DHSSPS code of practice
- The Computer Misuse Act 1990
- The Congenital Disabilities (Civil Liability) Act 1976
- The Consumer Protection (Northern Ireland) Order 1987
- The Control of Substances Hazardous to Health Regulations (Northern Ireland) 2003
- The Copyright, Designs and Patents Acts 1988
- The Data Protection Act (DPA) 1998
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- Data Protection (Subject Access Modification) (Health) Order 2000
- Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community Code Relating to Medicinal Products for Human Use as amended by Directive 2002/98/EC of the European Parliament and of the Council of 27 January 2003
- The Electronic Communications Act 2000
- The Environmental Information Regulations 2004
- The Foster Placement (Children) Regulations (Northern Ireland) 1996
- The Freedom of Information Act (FOIA) 2000
- The Gender Recognition Act 2004

- The Gender Recognition (Disclosure of Information) (England, Wales and Northern Ireland) (No. 2) Order 2005
- The Health & Personal Social Services, General Dental Services (Amendment) Regulations (Northern Ireland) 2008
- The Health & Personal Social Services, General Medical Services Contracts Regulations (Northern Ireland) 2004
- The Health and Safety at Work (Northern Ireland) Order 1978
- The Health and Social Services (Reform) Act (Northern Ireland) 2009
- The Human Fertilisation and Embryology Act 1990, as amended by the Human Fertilisation and Embryology Act 2008
- The Human Rights Act 1998
- The Human Tissue Act 2004
- The Limitation (Northern Ireland) Order 1989
- The Police and Criminal Evidence Act 1984:
- Police Act 1997 and the Memorandum to A Code of Practice for Third Party recipients of Criminal Record Information
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Public Health Act (Northern Ireland) 1967
- The Public Interest Disclosure (Northern Ireland) Order 1998
- The Public Records Act (Northern Ireland) 1923
- Disposal of Documents Order (Northern Ireland)1925
- The Radioactive Substances Act 1993
- The High-activity Sealed Radioactive Sources and Orphan Sources Regulations 2005
- The Re-use of Public Sector Information Regulations 2005
- The Safeguarding Vulnerable Groups (Northern Ireland) Order 2007
- The Sexual Offences (Amendment) Act 1992 (as amended by the Youth Justice and Criminal Evidence Act 1999)