

**SCOTTISH GOVERNMENT  
RECORDS MANAGEMENT:  
NHS CODE OF PRACTICE  
(SCOTLAND) Version 2.0  
March 2010**

## DOCUMENT CONTROL SHEET:

<b>Title:</b>	<i>Records Management: NHS Scotland Guidance</i>
<b>Date Published/Issued:</b>	31/03/2010
<b>Date Effective From:</b>	Date that document is effective from – especially important for policy and guidance documents
<b>Version/Issue Number:</b>	Version 2
<b>Document Type:</b>	Best Practice Guidance
<b>Document status:</b>	Final
<b>Author:</b>	Records Management Lead
<b>Owner:</b>	eHealth Directorate, Scottish Government
<b>Contact:</b>	Records Management Lead
<b>Target Audience</b>	Records Managers
<b>Supersedes</b>	<ul style="list-style-type: none"> <li>▪ SHM 58/60 – Scottish Hospital Service Destruction of Hospital Records;</li> <li>▪ ECS(A) 21/1969 – Disposal of Records That Have Lost Their Value;</li> <li>▪ MEL (1993) 152 – Guidance for the Retention and Destruction of Health Records;</li> <li>▪ HDL (2006) 28 – The Management; Retention and Disposal of Administrative Records;</li> <li>▪ CEL 28 (2008) - Records Management: NHS Code of Practice (Scotland)</li> </ul>

**Distribution:** This document has been distributed to

<b>Name:</b>	<b>Title/Organisation :</b>	<b>Date of Issue:</b>	<b>Version:</b>

# Contents

SCOTTISH GOVERNMENT RECORDS MANAGEMENT: NHS CODE OF PRACTICE (SCOTLAND) Version 2.0	March 2010	1
DOCUMENT CONTROL SHEET:		2
Contents		3
SECTION 1 – FOREWORD		6
Background		6
Aims		7
Types of Record covered by the Code of Practice		7
SECTION 2 – INTRODUCTION		9
General Context		10
Legal and Professional Obligations		13
NHS Scotland eHealth Strategy		14
Social Care Records		14
SECTION 3 – NHS RECORDS MANAGEMENT AND INFORMATION LIFECYCLE		15
Roles and Responsibilities for Records Management and Organisational Responsibility		15
Roles		16
Training		17
Policy and Strategy		18
Record Creation		19
Record Keeping		20
Record Maintenance – Storage Archiving and Scanning		21
Information Asset Register		24
Records Management Systems Audit		24
Information Quality Assurance		24
Disclosure and Transfer of Records		25
Retention and Disposal Arrangements		27
Appraisal of Records		28
Record Closure		29
Record Disposal		30
ANNEX A - GLOSSARY OF RECORDS MANAGEMENT TERMS		33
A		33

B - C .....	34
D .....	35
E .....	35
F - G .....	35
H .....	36
I .....	36
J .....	37
K - M .....	37
N .....	38
O- P .....	38
R .....	40
S .....	41
T .....	42
U - Z .....	42
ANNEX B - RESOURCES TO SUPPORT IMPROVEMENT .....	43
The Role of the Information Governance Framework and the Information Governance Toolkit .....	43
Other Reference Material .....	44
Useful Contacts .....	49
ANNEX C: LEGAL AND PROFESSIONAL OBLIGATIONS .....	52
Legislation contents .....	52
Other Obligations contents .....	53
Relevant Standards and Guidelines contents .....	54
Professional Codes of Conduct and Guidance .....	54
Legislation .....	55
Other obligations .....	88
Relevant standards and guidelines .....	93
Professional Codes of Conduct and Guidance .....	94
ANNEX D – ‘THE MANAGEMENT, RETENTION AND DISPOSAL OF PERSONAL HEALTH RECORDS .....	96
Introduction .....	96
Scope of Schedule .....	96
Responsibilities and Decision Making .....	97
Retention Periods .....	98
Disposal and Destruction of Personal Health Records .....	99

Decision Making .....	99
Disposal and Destruction .....	100
Archives .....	101
Interpretation of the Schedule .....	102
Health Records Retention Schedule .....	105
Pathology records: Documents, electronic and paper .....	116
Pathology Records: Specimens and Preparations. ....	121
Pathology Records: Transfusion Laboratories .....	124
Patient Held Records .....	126
Pharmacy Records: Prescriptions .....	127
Pharmacy Records: Clinical trials .....	127
Pharmacy Records: Worksheets .....	128
Pharmacy Records: Quality Assurance .....	129
Pharmacy Records: Orders .....	129
Pharmacy Records: Controlled Drugs, Others .....	130
Other Health Records .....	131
Principles to be used in Determining Policy Regarding the Retention and Storage of Essential Maternity Records .....	137
Joint Position on the Retention of Maternity Records .....	137
List of Maternity Records to be retained .....	138
<b>ANNEX E- ADMINISTRATIVE RECORDS RETENTION SCHEDULE ....</b>	<b>139</b>
Administrative Records - General .....	141
Administrative Records - Financial .....	143
Administrative Records - Property, Environment and Health & Safety .....	147
Administrative Records - Human Resource .....	151
Administrative Records - Procurement and Stores .....	153
Administrative Records - NHS Board .....	155
Administrative Records - Service Planning .....	158

# SECTION 1 – FOREWORD

## Background

1. The Records Management: NHS Code of Practice has been published by the Scottish Government eHealth Directorate as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in Scotland. It is based on current legal requirements and professional best practice.

2. The guidance was drafted in collaboration with a working group made up of representatives from the Scottish Government Health Directorate, Scottish NHS archivists, NHS Health Records Managers, patient groups and GP Practices. As part of its work, the working group commissioned a public consultation on the retention and disposal of health records in 2005. The results of that consultation have informed the drafting of this guidance. The draft was updated and issued for consultation during Autumn 2007. Further information can be found [here](#). The guidance has subsequently been reviewed and updated following the recommendations contained within the Strathmartine Report published in 2008 and requests from the service to incorporate the guidance and retention schedules for both Health Records and Administrative Records in to a single document.

3. Scotland's Clinical Governance and Risk Management standards are underpinned by information governance standards, to which Boards are supported in compliance by an electronic toolkit and knowledge portal. These standards make clear to Boards the requirements to be met on the management of patient and administrative records and freedom of information and data protection obligations, amongst other things. This Code provides a key component of these information governance arrangements. Further information regarding the National Information Governance standards relating to Health Records can be viewed via the Information Governance Specialist e-Library [here](#). This is an evolving document because standards and practice covered by the Code will change over time. It will therefore be subject to regular review and updated as necessary.

## **Aims**

4. The aims of this NHS Code of Practice are to:

- establish, as part of the wider information governance framework, records management best practice in relation to the creation, use, storage, management and disposal of NHS records;
- provide information on the general legal obligations that apply to NHS records;
- set out recommendations for best practice to assist in fulfilling these obligations, for example adhering to National Information Governance Standards;
- explain the requirement to select records for permanent preservation;
- set out recommended minimum periods for retention of NHS personal health records and administrative records regardless of the media on which they are held, and;
- indicate where further information on records management may be found;

## **Types of Record covered by the Code of Practice**

5. The following types of NHS records are covered by this retention schedule (including records of NHS patients treated on behalf of the NHS in the private health sector) regardless of the media on which they are held, including paper, electronic, images and sound) :

- personal health records (Paper based or electronic including those concerning all specialties, and GP medical records);
- records of private patients seen on NHS premises;
- records of blood and tissue donors;
- accident & emergency, birth, and all other registers;
- theatre registers & minor operations (and other related);
- x-ray and imaging reports, output and images;
- administrative records (including, for example, general, financial, property, environmental, health and safety, human resource, procurement/stores, NHS Board and service planning records).

**Annex D applies to personal health records and annex E to administrative records.**

**Please note:**

- sections **1, 2, 3, annex D** and **E** are for implementation;
- annexes **A, B** and **C** are to aid understanding and provide reference to other useful information;



## SECTION 2 – INTRODUCTION

6. The guidelines draw on advice and published guidance available from the Scottish Government Freedom of Information Unit and the National Archives of Scotland, and also from best practices followed by a wide range of organisations in both the public and private sectors. The guidelines provide a framework for consistent and effective records management that is standards based and fully integrated with other key information governance work areas.

7. This is an overarching Code of Practice on records management for Scottish NHS organisations. It incorporates references and links to previously published guidance and also takes cognisance of the recommendations accepted by the Cabinet Secretary for Health and Wellbeing in October 2008 following publication of the NHS QIS report in response to reports that person identifiable information had been found in disused buildings on the former Strathmartine Hospital in Tayside

8. NHS managers must demonstrate active progress in enabling staff to conform to the standards, identifying resource requirements and any related areas where organisational or systems changes are required. Information Governance performance assessment and management arrangements need to facilitate and drive forward the required changes. Those responsible for monitoring NHS performance, (e.g. NHS Quality Improvement Scotland -NHS QIS) will play a key role in ensuring that effective systems are in place.

9. The NHS is provided with support to deliver change through:

- Information Governance Standards, which can be viewed on the Specialist e-Library [here](#);
- Information Governance Toolkit;

NHS Scotland Information Governance Team and policy advisers in the Scottish Government eHealth Directorate. Further information on the above can be found in [Annex B](#).

## General Context

**10.** All NHS organisations are public authorities under Schedule 1 of the Freedom of Information (Scotland) Act 2002, and the records they create are subject to the Public Records (Scotland) Act 1937 (as amended). Scottish Ministers and all NHS organisations are obliged under Data Protection and Freedom of Information legislation to make arrangements for the safe keeping and eventual disposal of all types of their records. This is carried out under the overall guidance and supervision of the Keeper of the Records of Scotland who is answerable to the Scottish Parliament. Whilst this Code of Practice is based on the Scottish Government’s understanding of the relevant law in Scotland as at the date of publication, it is not, and should not be read as, a statement of the definitive legal position on any matter. NHS organisations should consult their own legal advisors for advice on any legal issues, which arise regarding the matters covered in this Code of Practice.

**11.** NHS organisations should seek advice from their Board’s own archivist on the management of records, particularly in relation to the permanent preservation of records. Where organisations do not have access to their own archivist, advice may be sought from the NHS Scotland archivists, or the National Archives of Scotland (see [Annex B](#) for further information).

**12.** Part one of the Freedom of Information (Scotland) Act 2002 Code of Practice on Records Management states:

“Records management should be recognised as a specific corporate function within the authority and should receive the necessary levels of organisational support to ensure effectiveness. It should bring together responsibilities for **all** records held by the authority, throughout their life cycle, from planning and creation through to ultimate disposition. It should have clearly defined responsibilities and objectives, and the resources to achieve them. It is desirable that the person, or persons, responsible for the records management function should also have either direct responsibility for, or a formal working relationship with, the person(s) responsible for freedom of information, data protection and other information management issues. Further information can be obtained [here](#).”

**13.** The Chief Executive has overall accountability for ensuring that records management operates legally within the Board. The Caldicott Guardian works in liaison with the organisation's Health Records Manager(s), Corporate Records Manager(s), Information and Communications Technology (eHealth) Manager(s), Information Governance Manager and others with similar responsibilities, to ensure there are agreed systems for records management including managing the confidentiality and security of information and records within their organisation. NHS organisations are also required to take positive ownership of, and responsibility for, the records legacy of predecessor organisations and/or obsolete services.

**14.** In addition, NHS organisations need robust records management procedures to meet the requirements set out under the Data Protection Act 1998, the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004.

**15.** Records are a valuable resource because of the information they contain. High quality information underpins the delivery of high quality evidence based health care, accountability, clinical and corporate governance 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 service ensures that information is properly managed and is available whenever and wherever there is a justified need for information, and in whatever media it is held or required to:

- support patient care and continuity of care;
- 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 NHS services;
- meet legal requirements, including requests from patients or other individuals under subject access legislation or Freedom of Information;
- assist clinical and other audits;
- support improvements in clinical effectiveness through research and also support archival functions by taking account of the historical importance of material and the needs of future research;

- support patient choice and control over treatment and services designed around patients.

**16.** Effective records management also supports operational efficiency by reducing the time taken to identify and locate information, minimising duplication of records and confusion over version control and significant savings in physical and electronic space.

**17.** This Code of Practice, together with the supporting Annexes identifies the specific actions, managerial responsibilities, and recommended retention periods (in line with the 5th principle of the Data Protection Act 1998) for the effective management of all NHS records, from creation, as well as day-to-day use of the record, storage, maintenance and ultimate disposal.

**18.** All individuals who work for an NHS organisation are responsible for any records, which they create, or use in the performance of their duties. Furthermore, any record that an individual creates is subject to the Public Records (Scotland) Act 1937 (as amended), and the information contained in such records is subject to the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004. There is a specific requirement under Regulation 4 of the Act on a public authority to take reasonable steps to organise and keep up to date the environmental information relevant to its functions which it holds and at least the types of information detailed in Reg 4 (2). [Annex C](#) contains further information on legal and professional obligations.

## Legal and Professional Obligations

**19.** Another key statutory requirement for compliance with records management principles is the Data Protection Act 1998. It provides a broad framework of general standards that have to be met and considered in conjunction with other legal obligations. The Act regulates the processing of personal data, held manually and on computer. It applies to personal information generally, not just to health records. Therefore the same principles apply to personal data relating to staff, contractors, volunteers, students and other individuals who work in or have dealings with NHS Scotland.

**20.** 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. It therefore includes such items of information as name, address, age, race, religion, gender and physical, mental or sexual health.

**21.** Processing includes everything done with that information, i.e. holding, obtaining, recording, using, disclosure, sharing, disposal, transfer or destruction.

More information on the application of the Data Protection Act is contained in [Annex C](#)

**22.** Other legislation relating to personal and corporate information and the records management function generally can also be found in [Annex C](#). Additionally, clinicians are under a duty to meet record keeping standards set by their regulatory and professional bodies.

## **NHS Scotland eHealth Strategy**

**23.** The eHealth programme aims to ensure a complete health record is available at the point of need in NHS Scotland. The success of this will depend on many factors, and good records management will be essential to ensure paper and electronic records are managed consistently. Further information is available [here](#)

## **Social Care Records**

**24.** Social Care Records Management is outside the scope of this Code of Practice. However, the Scottish Government Transformational Technologies Division has developed joint national data standards for use in eCARE. The increase in joint working from this initiative means that although outwith scope this Code of Practice is generally applicable to all organisations, and colleagues from social care organisations are encouraged to adopt similar standards of practice.

## **SECTION 3 – NHS RECORDS MANAGEMENT AND INFORMATION LIFECYCLE**

**25.** Records and information are considered to have a “lifecycle” from creation or receipt in the organisation, throughout the period of its ‘active’ use, then into the period of ‘inactive’ retention, (such as closed files which may still be required occasionally) and then finally to either confidential disposal or (for a very small proportion) permanent preservation in an archival facility.

**26.** A similar “information lifecycle” approach applies to managing the flow of an information system’s data and associated metadata from creation and initial storage to the time when it becomes obsolete and is deleted.

### **Roles and Responsibilities for Records Management and Organisational Responsibility**

**27.** The records management function should be recognised as a specific corporate responsibility within every NHS 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 ultimate disposal. It should have clearly defined responsibilities and objectives, and necessary resources to achieve them.

**28.** Designated members of staff of appropriate seniority (i.e. Board level or reporting directly to a Board member) should have lead responsibility for corporate and health records management within the organisation. The model within each Health Board may differ dependent on local accountability. This lead role should be formally acknowledged and made widely known throughout the organisation.

**29.** The manager, or managers, responsible for the records management function should be directly accountable to, or work in close association with the manager or managers responsible for Freedom of Information, Data Protection and other information governance issues as well as the Medical Director who is operationally accountable for the quality of clinical information contained within personal health records in the organisation.

30.

## Roles

**The NHS Board:** is responsible for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

**The Chief Executive:** has overall responsibility for records management in the NHS Board. As accountable officer he /she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records Management is key to this as it will ensure appropriate, accurate information is available whenever required.

**The Caldicott Guardian:** has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

**The Health Records Manager:** is responsible for the overall development and maintenance of health records management practices throughout the organisation. They have particular responsibility for drafting guidance to support good records management practice in relation to clinical records and for promoting compliance with this Records Management – Code of Practice, in such a way as to ensure the efficient, safe, appropriate and timely retrieval of patient information.

**The Corporate Records Manager:** is responsible for the overall development and maintenance of corporate and administrative records management practices throughout the organisation. They have particular responsibility for drafting guidance to support good records management practice (other than for clinical records) and for promoting compliance with this Records Management – Code of Practice.



**Local Records Management Co-ordinators**: The responsibility for records management at directorate or departmental level is devolved to the relevant directors, directorate and departmental managers. Senior managers of units and business functions within the NHS Board have overall responsibility for the management of records generated by their activities in compliance with the NHS Board's records management policy. Local Records Management Co-ordinators may be designated to support the Health and Corporate Records Manager(s) to oversee local implementation and compliance.

**All Staff:**

All NHS staff , whether clinical or administrative, who create, receive and use documents and records have records management responsibilities. All staff must ensure that they keep appropriate records of their work and manage those records in keeping with the Records Management –Code of Practice and the relevant policies and guidance within their Board.

**Training**

31. All staff, whether clinical or administrative, must be appropriately trained so that they are fully aware of their personal responsibilities as individuals with respect to record keeping and management, and that they are competent to carry out their designated duties. This should include training for staff in the use of electronic records systems. It should be done through both generic and specific training programmes, complemented by organisational policies and procedures and guidance documentation. For example, Health Records Managers who have lead responsibility for personal health records and the operational processes associated with the provision of a comprehensive health record service should have up-to-date knowledge of, or access to expert advice on, the laws, guidelines, standards and best practice relating to records management and informatics.

## **Policy and Strategy**

**32.** Each NHS organisation should have in place an overall policy statement, endorsed by the Board and made readily available to staff at all levels of the organisation on induction and through regular update training, on how it manages all of its records, including electronic records

**33.** The policy statement should provide a mandate for the performance of all records and information management functions. In particular, it should set out an organisation's commitment to create, keep and manage records and document its principal activities in this respect.

**34.** The policy should also:

- outline the purpose of records management within the organisation, and its relationship to the organisation's overall strategy;
- define roles and responsibilities within the organisation including the responsibility of individual NHS staff to document their actions and decisions in the organisation's records, and to dispose of records appropriately when they are no longer required;
- define roles, responsibilities and procedure for safe transfer, storage or confidential disposal of records when staff leave an organisation, or when NHS Board premises are being decommissioned;
- define the process of managing records throughout their life cycle, from their creation, usage, maintenance and storage to their ultimate destruction or permanent preservation;
- provide a framework for supporting standards, procedures and guidelines; and
- indicate the way in which compliance with the policy and its supporting standards, procedures and guidelines will be monitored and maintained.

**35.** The policy statement should be reviewed at regular intervals (a minimum of once every 3 years or sooner if new legislation, codes of practice or national standards are introduced) and, if appropriate, it should be amended to maintain its currency and relevance.

## **Record Creation**

**36.** Each operational unit (for example Finance, Estates and Facilities, eHealth, Human Resources, Direct Patient Care) of an NHS organisation should have in place procedures for documenting its activities. This process should take into account the legislative and regulatory environment in which the unit operates.

**37.** Records of operational activities should be complete and accurate in order to allow employees and their successors to undertake appropriate actions in the context of their responsibilities, to facilitate an audit or examination of the organisation by anyone so authorised, to protect the legal and other rights of the organisation, its patients, staff and any other people affected by its actions, and provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative. Appropriate version control arrangements that support the management of multiple revisions to the same document should be in place.

**38.** Records created by the organisation should be arranged in a record-keeping system that will enable the organisation to obtain the maximum benefit from the quick and easy retrieval of information while having regard to security.

**39.** Not all documents created or received by NHS employees in the course of their work need to be held in the record-keeping system. For example, most emails are of only passing value and can be deleted as soon as they have been read or actioned. (emails, which contain significant information or instructions, should be retained as appropriate within the record-keeping system.) Many circulars and routine correspondence can be destroyed once read.

## Record Keeping

**40.** Implementing and maintaining an effective records management service depends on knowledge of what records are held, where they are stored, who manages them, in what form(s) they are made accessible, and their relationship to organisational functions (e.g. Finance, Estates, IT, Direct Patient Care). An information survey or record audit is essential to meeting this requirement. The survey will provide a description of the record collection along with its location and details of the responsible manager. This helps to promote control over the records, and provides valuable data for developing records appraisal and disposal policies and procedures.

**41.** 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 documentation should provide an administrative context for effective management of the records.

**42.** The record keeping system, whether paper or electronic, should include a documented set of rules for referencing, 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.

**43.** Records should be structured within an organisation-wide corporate “Fileplan” which reflects the functions and activities of the organisations and facilitates the appropriate sharing and effective retrieval of information.

**44.** Where records are kept in electronic form, wherever possible they should be held within an Electronic Document and Records Management System (EDRMS) which conforms to the standards of the European Union “Model Requirements” (MoReq). Find more details [here](#)

**45.** Where an EDRMS is not yet available, electronic documents should be stored on shared, network servers in a clear and meaningful folder structure. The folder structure should reflect the organisation’s fileplan in the same way as paper files, which represent the functions and activities of the organisation or unit. The server should be subject to frequent back-up procedures in line

20

with the NHS Information Security Policy. Users should apply the functionality of the relevant software to protect electronic documents against inappropriate amendment (for example, by password protecting documents.) Please note: It is almost impossible to fully protect documents in a non-EDRMS environment, or provide full audit and authenticity evidence.

## **Record Maintenance – Storage Archiving and Scanning**

**46.** The NHS organisation should put in place robust procedures to manage control of access, retrieval and use of records to ensure continued integrity, reliability and authenticity of the records as well as their accessibility for the duration of their retention until the time of their ultimate disposal. The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions. The record-keeping system should also address the management of emails, including aspects such as the titling of emails and the handling of email attachments.

**47.** Storage accommodation for current paper records should be clean and tidy, allow adequate space for expansion, prevent damage to the records and provide a safe working environment for staff.

**48.** For records in digital format, maintenance in terms of back-up and planned migration to new platforms should be designed and scheduled to ensure continuing access to accurate, reliable and readable records.

**49.** Equipment used to store current records on all types of media should provide storage that is safe and secure from unauthorised access and meets health and safety and fire regulations, but which also allows maximum accessibility to the information commensurate with its frequency of use. Storage equipment should be as space-efficient as possible.

**50.** When paper records are no longer required for the conduct of current business, their placement in a designated secondary storage area may be a more economical and efficient way to store them. Procedures for handling records should take full account of the need to preserve important information and keep it confidential and secure. There should be policies and procedures in place for managing the lifecycles of both paper and electronic records.

51. A contingency or business continuity plan should be in place to provide protection for all types of records that are vital to the continued functioning of the organisation. Key expertise in relation to environmental hazards, assessment of risk, business continuity and other considerations is likely to rest with information security staff and their advice should be sought on these matters.

52. NHS organisations may consider the option of scanning into electronic format, records which exist in paper format, for reasons of business efficiency. Where this is proposed, the factors to be taken into account include:

- 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 need to consult in advance with NHS archivists or the National Archives of Scotland with regard to records which may have archival value, as the value may include the form in which it was created; and
- the need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the [“Evidential Weight and Legal Admissibility of Information Stored Electronically”](#) (BIP 0008-1:2008) and the [Document Scanning: Guide to Scanning Business Documents](#) (PD 0016:2001) which provides guidance to evaluate scanners to user requirements

53. The scanning process should be considered to have at least 4 stages to convert documents into ready to use electronic images. These are as follows:

**Document preparation:** Document preparation in advance of scanning is often needed, and should be taken into consideration as part of the whole process. It covers jobs such as removing staples, unfolding or unrolling, removing documents from binders and so on. There may also be a need to redo these jobs after scanning if the documents are to be retained.

**Data capture:** Data capture is the conversion of the document from readable format into electronic format. This is scanning but is only a part of the scanning process.

**QA (Quality Assurance):** At its most basic level the QA process should check the quality of the image and verify that all documents have been scanned. Image quality is often checked on a sampling basis, perhaps checking the first and last image in a batch. The number of sheets can be compared to the number of image files produced to verify that all the documents have been scanned. Scanners with endorsing features can make this easier by marking the documents as they feed through the scanner. Test target can also be used to check that output quality of scan has been maintained by comparison with hard copy kept for this purpose.

**Indexing:** After the image is captured as a computer file, there needs to be a way to search for that scanned images from the computer system. In effect the document needs to be filed or indexed in a database.

The way in which a document is to be retrieved in the future should be used to define the indexing data fields. Examples might be patient demographic data, an invoice or account number, or the name and address of someone who sent the letter.

The indexing of documents received from outside sources generally involves keyboard data entry. In-house documents can be designed to benefit from forms processing, text recognition and bar code reading techniques to cut this indexing overhead.

**54.** In order to fully realise business efficiency, organisations should consider securely disposing of paper records that have been copied into electronic format and stored in accordance with appropriate standards and the need to dispose of records in accordance with the retention schedule. Advice should be sought from the organisation's Records Manager(s) or Information Governance Manager, NHS Scotland Archivists or the National Archives of Scotland. It is rarely cost-effective to retrospectively scan non-current paper records as an alternative to low-cost secondary storage.

## Information Asset Register

**55.** Each NHS organisation should establish and maintain an Information Asset Register. Mechanisms should be established through which departments can register records and media containing business or personal identifiable information they are maintaining. The inventory should provide a description of the record collection along with its location and details of the responsible manager. The register should be reviewed annually. Further information can be found in Records Management Guidance **Note 004** [here](#).

## Records Management Systems Audit

**56.** The NHS organisation will regularly audit its records management practices for compliance with this Records Management – Code of Practice. Results of audits will be reported to the NHS Board through the appropriate committee.

## Information Quality Assurance

**57.** It is important that all NHS organisations train staff appropriately and provide regular update training. Training and guidance in record-keeping appropriate to the role should be an integral part of induction and training procedures. In the context of records management and information quality, organisations need to ensure that their staff are fully trained in record creation and maintenance, including having an understanding of:

- what they are recording and how it should be recorded;
- why they are recording it;
- how to validate information with the patient or carers or against other records – so staff are recording the correct data;
- how to identify and correct errors – so that staff know how to correct errors and how to report errors if they find them;
- and the use of information – so staff understand what the records are used for (and therefore why accuracy is so important);
- how to update information and add in information from other sources.



## **Disclosure and Transfer of Records**

**58.** There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties, and similarly, a range of provisions that require or permit disclosure. The key statutory requirements can be found in [Annex C](#).

**59.** In particular, information relating to living individuals is covered by the principles of Data Protection and include a statutory right for individuals to access their personal data and to have factual inaccuracies corrected. The Freedom of Information (Scotland) Act 2002 confers a statutory right of access to deceased person's health records only after a period of 100 years. Notwithstanding, it may be possible to put in place mechanisms that both safeguard patient confidentiality and enable controlled access to health records of the deceased within this 100- year time limit. In general confidentiality of records particularly relating to patients, staff or students should be maintained for 75 years (100 years for minors) from the beginning of the calendar year following the date of the last entry of the record.

**60.** In Health Boards the Caldicott Guardian, supported by the Health Records Manager(s) and Data Protection Officer should be involved in any proposed disclosure of confidential patient information, informed by the Scottish Government Health Directorates publication 'Code of Practice on Protecting Patient Confidentiality'. This can be downloaded [here](#). In GP surgeries, the responsibility for making decisions about disclosure ultimately rests with the GP. For patients, a leaflet has been produced by Health Rights Information Scotland (HRIS) called 'How to see your Health Records'. It provides patients with information on how to make a subject access request to view their health records. The leaflet can be downloaded [here](#)

**61.** 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 NHS Scotland Information Security policy and standards sets out the requirements for the storage and transmission of corporate and personal records. More information can be found [here](#)

**62.** To comply with the Data Protection Act 1998, the Human Rights Act 1998 and to conform with the Caldicott principles, it is necessary to ensure data which can be linked to an individual, (either patient, client or staff member) is transported in a secure manner. Transportation methods employed must be fit for purpose and in accordance with the procedures of each individual department. A number of methods may be employed for manual and electronic records:

Manual:

- Single record envopak carriers with seals
- Multiple record envopak carriers with seals
- Non-tearable textured envelopes
- Purpose designed plastic boxes with seals
- Lockable pilot bags

Electronic:

Refer to local NHS Board policy for secure electronic transfer of data and use of mobile devices. Further information can be found [here](#).

Docman transfer enables GP Practices to transfer all relevant scanned patient documents to the next GP Practice electronically, when a patient transfers GP Practice, and also to receive electronic patient documents for importing in to Docman. Further information can be found [here](#).

**63.** Privacy marking should always be used on packages, carriers and purpose designed boxes used to transport records, documents or media containing person, identifiable information.

- ‘Confidential – Clinical Information’ – for all patient identifiable information of a clinical nature.
- ‘Confidential – Personal Information’ – for person, identifiable information which should be opened by the addressee only.

**64.** There are also a range of guidance documents (e.g. the UK Information Commissioner’s Use and Disclosure of Health Information) that interpret statutory requirements and there may be staff within organisations that have special expertise in, or can advise on, particular types of disclosure. In particular, organisations should be aware of the Freedom of Information

(Scotland) Act 2002 Code of Practice on Records Management November 2003 (laid before the Scottish Parliament on 10th November 2003 pursuant to Section 61(6) of the Freedom of Information (Scotland) Act 2002, and prepared in consultation with the Scottish Information Commissioner and the Keeper of the Records of Scotland). See [Annex C](#)

## **Retention and Disposal Arrangements**

**65.** The term retention and disposal relates to the actual processes of retention and disposal of records throughout their lifecycle (i.e. primary storage, secondary storage, microform, scanning, summarising, archiving and confidential destruction)

**66.** Detailed guidance for retention and disposal of personal health records can be found in [Annex D](#).

**67.** Detailed guidance for retention and disposal of administrative records can be found in [Annex E](#).

**68.** 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 an archive 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.

**69.** The design of databases and other structured information management systems must include the functionality to dispose of time-expired records. Databases should be subject to regular removal of non-current records in line with the organisation's retention schedule.

**70.** Each NHS organisation should have a dated documented policy which has been written/reviewed within the last three years, for the retention, archiving or destruction of the organisations records in accordance with this Records Management – Code of Practice. The policy should be ratified by the Board or by an appropriately delegated committee of the Board for example the Health Records, Information Governance or Clinical Governance Committee. The schedules should cover all series of records held, in any media, and should state the agreed retention period and disposal action, including, where

appropriate, an indication of those records which should be considered for archival preservation.

**71.** The records policy document should contain detailed guidance of the process to be followed to ensure complete clearance and removal of business documents, health records or documents containing person identifiable information whenever NHS premises are being decommissioned. Further information can be found in Records Management Guidance Note Number 008.

## **Appraisal of Records**

**72.** Appraisal refers to the process of determining whether records are worthy of permanent archival preservation. This should be undertaken in consultation with the organisations own Archivist, or with a local authority or university archive where there is an existing relationship. Three NHS Boards in Scotland employ archivists: Grampian (which also provides a service to NHS Highland), Lothian and Glasgow. Each collects, lists and preserves corporate and health records of and relating to NHS organisations and predecessor bodies and institutions in their local area. Some Boards, including Tayside and Ayrshire and Arran, have made arrangements with their local archives for the storage and management of records. Alternatively advice can be sought from the National Archives of Scotland (NAS), particularly in the case of Special Boards who should deposit archives of permanent value with the NAS as they advise.

**73.** Procedures should be put in place in all NHS organisations to ensure that appropriately trained personnel appraise records at the appropriate time. The purpose of this appraisal process is to ensure that the records are examined at the appropriate time to determine whether or not they are worthy of archival preservation, whether they need to be retained for a longer period as they are still in use, or whether they should be destroyed. In the majority of cases, appraisal will apply to the entire series of records and can be included in the records retention policy, rather than being conducted on individual records.

**74.** It is important when reviewing records that their long term historical and research value is taken in to account. Records which document the history and development of the organisation and important policy decisions, such as board or committee minutes, annual reports, policy and strategy documents

and major departmental reports and investigations should be considered. In addition sample of patient files and older registers and ward journals are valuable for historical medical and social research. Note that no surviving personal health or administrative record dated 1948 or earlier should be destroyed.

**75.** Where there are records that have been omitted from the retention schedules, or when new types of records emerge, the Scottish Government eHealth Directorate and/or an NHS archivist should be consulted. The National Archives of Scotland can also provide advice about records requiring permanent preservation.

**76.** All NHS organisations must have procedures in place for recording the disposal decisions made following appraisal. An assessment of the volume and nature of records due for appraisal, the time taken to appraise records, and the risks associated with destruction or delay in appraisal will provide information to support an organisation's resource planning and workflow. The Records Manager in the NHS organisation should determine the most appropriate person(s) to carry out the appraisal in accordance with the retention schedule. This should be a Manager with appropriate seniority, training and experience who has an understanding of the subject area to which the record relates.

## **Record Closure**

**77.** Records should be closed (i.e. made inactive and transferred to secondary storage) as soon as they have ceased to be in active use other than for reference purposes. An indication that a file of paper records or folder of electronic records has been closed together with the date of closure, should be shown on the record itself as well as noted in the index or database of the files/folders. Where possible, information on the intended disposal of electronic records should be included in the metadata when the record is created.

**78.** The storage of closed records should follow accepted standards relating to environment, security and physical organisation of the files.

## Record Disposal

**79.** Each organisation must have a retention/disposal policy that is based on the retention schedules referred to in paragraphs 66 and 67 of this Code of Practice. The policy should be supported by, or linked to the retention schedules, which should cover all records created, including electronic records. Schedules should be arranged based on series or collection of records and should indicate the appropriate disposal action for all records. Schedules should clearly specify the agreed retention periods, which must be based on the retention schedules referred to in paragraphs 66 and 67 of this Code of Practice, for the organisation.

**80.** Records selected for archival preservation and no longer in regular use by the organisation should be transferred as soon as possible to an archive. No surviving personal health or administrative record dated 1948 or earlier should be destroyed.

**81.** Good practice suggests that non-active records should be transferred no later than 30 years from creation of the record, with electronic records being transferred within a shorter period.

**82.** Records (including copies) not selected for archival preservation and which have reached the end of their administrative life should be destroyed in as secure a manner as is appropriate for the level of confidentiality or protective markings they bear. This can be undertaken on site or via an approved contractor. Confidential records should be destroyed in accordance with BS EN 15713:2009 – Secure Destruction of Confidential Material - Code of Practice. It is the responsibility of the NHS organisation to ensure that the methods used throughout the destruction process provide appropriate safeguards against the accidental loss or disclosure of the contents of the records at every stage. Accordingly, contractors should be required to sign confidentiality undertakings and to produce written certification as proof of destruction. There is a common law duty of confidence to patients and employees as well as a duty to maintain professional ethical standards of confidentiality. This duty of confidence continues even after the death of the patient or an employee or contractor has left the NHS.

**83.** Many NHS records, including corporate 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. The methods used to destroy records must be fully effective and secure their complete illegibility. Destruction by shredding or pulping is preferable. If the hospital or NHS organisation has no immediate access to an industrial shredder there are numerous firms that can provide this service. Recycling is an alternative option but this should only be considered for non-person identifiable or non sensitive business documents, otherwise the records should be shredded before being sent for recycling. This can be done on site or via an approved contractor.

**84.** It is important to have destruction as well as preservation policies for electronic records. It is often helpful that an expert can retrieve deleted files in an emergency, but this ability to retrieve deleted electronic data has inherent dangers for confidential information when hardware and software is discarded. It may also jeopardise the viability of a records management programme if records that are supposedly 'destroyed' can be retrieved from the system. If hardware or software is to be discarded advice must be sought from the relevant IT Security Officer.

**85.** It is essential that the destruction process is documented. The following information should be recorded 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.

- Description of record
- Reference number if applicable
- Number of records destroyed
- Date of destruction
- Who authorised destruction
- Who carried out the process
- Reason for destruction (this should refer to the retention/disposal policy)

**86.** Whenever patient/client records are being destroyed the relevant Master Patient Index should be updated with the date of destruction so that this is immediately known should the patient/client represent to the service or make an enquiry for access to their health records.

**87.** Records should not be destroyed before the end of the period stated in the Records Management - Code of Practice Annex [D](#) and [E](#). These periods reflect the statutory time limits for legal action to be taken. Any NHS Board which ignores these minimum periods would be in breach of guidelines laid down by Scottish Government, and would run the risk of being unable to defend itself against claims for alleged medical negligence.

**88.** 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 (Scotland) Act have been exhausted or the legal process completed.



# ANNEX A - GLOSSARY OF RECORDS MANAGEMENT TERMS

**Note:** The National Archives of the United Kingdom publishes standards, guidance and toolkits on the management of public records in all formats. These standards reflect the legislative and administrative arrangements, which apply to UK public records. However, in so far as they are applicable to Scotland, they contain helpful practical advice, which is commended to Scottish public authorities.

## A

### **Access**

The availability of, or permission to consult, records. (The National Archives, Records Management Standard RMS1.1)

### **Appraisal**

The process of evaluating an organisation's activities to determine which records should be kept, and for how long, to meet the needs of the organisation, the requirements of Government accountability and the expectations of researchers and other users of the records. (The National Archives, Records Management Standard RMS 1.1)

### **Archives**

Those records that are appraised as having permanent value for evidence of ongoing rights or obligations, for historical or statistical research or as part of the corporate memory of the organisation. Those records that are appraised as having permanent value. (The National Archives, Records Management Standard RMS 3.1)

### **Authenticity**

An authentic record is one that can be proven:

To be what it purports to be

- To have been created or sent by the person purported to have created or sent it, and
- To have been created or sent at the time purported

To ensure the authenticity of records, organisations should implement and document policies and procedures which control the creation, receipt,

transmission, maintenance and disposition of records to ensure that records creators are authorised and identified and that records are protected against unauthorised addition, deletion, alteration, use and concealment. (BS ISO 15489-1:2001(E))

## **B - C**

### **CHI Number**

The CHI ('Community Health Index') number is a unique numeric identifier, allocated to each patient on first registration with the system. It is a 10-character code consisting of the 6-digit date of birth (DDMMYY), two digits, a 9th digit, which is always even for females and odd for males, and an arithmetical check digit. It is a key component in the implementation of an Electronic Patient Record in Scotland.

### **Classification**

The systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system. (BS ISO 15489-1:2001(E))

### **Conversion (See Also Migration)**

The process of changing records from one medium to another, or from one format to another. (BS ISO 15489-1:2001(E))

### **Corporate Records**

Records (other than health records) that are of, or relating to, an organisation's business activities covering all the functions, processes, activities and transactions of the organisation and of its employees.

### **Current Records**

Current records are those records necessary for conducting the current and on-going business of an organisation.

## **D**

### **Destruction**

The process of eliminating or deleting records beyond any possible reconstruction. (BS ISO 15489-1:2001(E))

### **Disposal**

Disposal is the implementation of appraisal and review decisions. These comprise the destruction of records and the transfer of custody of records (including the transfer of selected records to an archive institution). They may also include the movement of records from one system to another (for example, paper to electronic). (The National Archives, Records Management Standard RMS1.1)

### **Disposition**

A range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments. (BS ISO 15489- 1:2001(E))

## **E**

### **Electronic Record Management System**

A system that manages electronic records throughout their lifecycle, from creation and capture through to their disposal or permanent retention, and retains their integrity and authenticity while ensuring that they remain accessible.

## **F - G**

### **File**

An organised unit of documents grouped together either for current use by the creator or in the process of archival arrangement, because they relate to the same subject, activity or transaction. A file is usually the basic unit within a records series.

An accumulation of records maintained in a predetermined physical arrangement. Used primarily in reference to current records. (The National Archives, Records Management Standard RMS 1.1)

## **Filing System**

A plan for organising records so that they can be found when needed. (The National Archives, Records Management Standard RMS 1.1)

## **H**

### **Health Record**

The health record is a single record with a unique identifier, which is a composite of all data on a given patient. It contains information relating to the physical or mental health of an individual who can be identified from that information and which has been recorded by, or on behalf of, a health professional, in connection with the care of that individual. This may comprise text, sound, image and/or paper and must contain sufficient information to support the diagnosis, justify the treatment and facilitate the on-going care of the patient to which it refers.

## **I**

### **Indexing**

The process of establishing access points to facilitate retrieval of records and/or information. (BS ISO 15489-1:2001(E))

### **Information Audit**

An information audit looks at the means by which an information survey will be carried out and what the survey is intended to capture.

### **Information Survey/Records Audit**

An information survey or records audit is the comprehensive gathering of information about records created or processed by an organisation. It helps an organisation to promote control over its records, and provides valuable data for developing records appraisal and disposal procedures. It will also help an organisation to:

- Identify where and when records are generated and stored within the organisation and how they are ultimately disposed of;
- Accurately chart the current situation in respect of records storage and retention organisation-wide, to make recommendations on the way forward and the resource implications to meet existing and future demands of the records management function.

## **Integrity of Records**

The integrity of a record refers to its being complete and unaltered. It is necessary that a record be protected against unauthorised alteration. Records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorised and who is authorised to take them. Any unauthorised annotation, addition or deletion to a record should be explicitly indicated and traceable.

## **J**

### **Jointly Held Records**

Where a record is jointly held by health and social care professionals, e.g. in an Integrated Health and Social Care Community Mental Health Team (CMHT), it should be retained for the longest period for that type of record. That is, if social care has a longer retention period than health, the record should be held for the longer period.

## **K - M**

### **Metadata**

Contextual information about a record. Data describing context, content and structure of records and their management through time. Metadata is structured information that enables us to describe, locate, control and manage other information. Metadata can be broadly defined as "data about data". Metadata is defined in ISO 15489 as: data describing context, content and structure of records and their management through time. It refers to the searchable definitional data that provides information about or documentation of other data managed within an application or environment. For example, a library catalogue, which contains data about the nature and location of a book, is data about the data in the book.

Therefore, metadata should include (amongst other details) elements such as the title, subject and description of a record, the creator and any contributors, the date and format. For further information, see The National Archives: Metadata Standard [here](#)

The e-Government Metadata Standard (e-GMS) lays down the elements refinements and encoding schemes to be used by government officers when creating metadata for their information systems. The e-GMS forms part of the e-Government Information Framework (e-GIF). The e-GMS is required to ensure maximum consistency of metadata across public sector organisations. Find out more [here](#)

### **Microform**

Records in the form of microfilm or microfiche, including aperture cards.

### **Migration (See Also Conversion)**

The act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and usability. (BS ISO 15489-1:2001(E))

### **Minutes (Master Copies)**

Master copies are the copies held by the secretariat of the meeting, i.e. the person or department who actually takes the minutes, writes them and issues them.

### **Minutes (Reference Copies)**

Copies of minutes held by individual attendees at a given meeting.

## **N**

### **NHS Records**

All NHS organisations are public authorities under Schedule 1 of the Freedom of Information (Scotland) Act 2002. The records created and used by all NHS employees are subject to the terms of the Public Records (Scotland) Act 1937 (as amended). The information contained in those records is subject to Data Protection and Freedom of Information legislation. Health records are the most important tool to support patient care and continuity of that care.

## **O- P**

### **Paper Records**

Records in the form of files, volumes, folders, bundles, maps, plans, charts, etc.

## **Permanent Retention**

Corporate and health records will not normally be retained for longer than the specified retention period. However a selection of records of long-term legal, administrative, epidemiological and/or historical value should be identified for permanent preservation. Such records should be transferred to an archive, either the organisation's own NHS archive or a local authority or university archive with which the organisation has an existing relationship.

Section 33 of the Data Protection Act permits personal data identified as being of historical or statistical research value to be kept indefinitely as archives.

## **Preservation**

Processes and operations involved in ensuring the technical and intellectual survival of authentic records through time. (BS ISO 15489-1:2001(E))

## **Protective Marking**

The process of determining security and privacy restrictions on records.

## **Publication Scheme**

A publication scheme is required of all NHS organisations under the Freedom of Information (Scotland) Act. It details information, which is available to the public now or will be in the future where it can be obtained from and the format it is available in. Schemes must be approved by the Scottish Information Commissioner and should be reviewed periodically to make sure they are accurate and up to date.

## **Public Records (Scotland) Act 1937**

For information, including the text of the Act, see the National Archives of Scotland website [here](#).

## **Records**

Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations, or in the transaction of business. (BS ISO 15489.1) An NHS record is anything, which contains information (in any medium) which has been created or gathered as a result of any aspect of the work of NHS employees - including consultants, agency or casual staff.

## R

### **Records Management**

Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. (BS ISO 15489-1:2001(E))

### **Record Series**

Documents arranged in accordance with a filing system or maintained as a unit because they result from the same accumulation or filing process, or the same activity; have a particular form; or because of some other relationship arising out of their creation, receipt or use. (International Council on Archives' (ICA) General International Standard Archival Description or ISAD(G). Find out more [here](#)

### **Record System/Record-Keeping System**

An information system which captures, manages and provides access to records through time. (The National Archives, Records Management: Standards and Guidance - Introduction Standards for the Management of Government Records). Records created by the organisation should be arranged in a record-keeping system that will enable the organisation to obtain the maximum benefit from the quick and easy retrieval of information. Paper and electronic record-keeping systems should contain descriptive and technical documentation to enable the system and the records to be understood and to be operated efficiently, and to provide an administrative context for effective management of the records. The record-keeping system, whether paper or electronic, should include a documented set of rules for referencing, titling, indexing and, if appropriate, the protective marking of records. These should be easily understood to enable the efficient retrieval of information and to maintain security and confidentiality.

### **Redaction**

The process of removing, withholding or hiding parts of a record due to the application of a Freedom of Information exemption.



## **Registration**

Registration is the act of giving a record a unique identifier on its entry into a record-keeping system.

## **Retention**

The continued storage and maintenance of records for as long as they are required by the creating or holding organisation until their disposal, according to their administrative, legal, financial and historical evaluation.

## **Review**

The examination of records to determine whether they should be destroyed, retained for a further period, or transferred to an archive.

## **S**

### **Scottish Information Commissioner (See Also UK Information Commissioner)**

The Scottish Information Commissioner enforces and promotes the Freedom of Information (Scotland) Act 2002

### **Scottish NHS Archivists**

Three NHS Boards in Scotland employ archivists: Grampian (which also provides an archive service to NHS Highland), Lothian, and Glasgow. The funding and managerial arrangements for each of these archives differs, but each collects, lists and preserves corporate and health records of and relating to the NHS organisations and predecessor bodies and institutions in their local area. NHS organisations which do not employ their own Archivist are welcome to contact one of the NHS Archivists for advice and information on records management and archiving. See Annex B for further details. These organisations may wish to make their own arrangements with local authority or university archives for the transfer of records selected for permanent preservation; such arrangements require the agreement of the Keeper of the Records of Scotland.

The Health Archives and Records Group (HARG) is a representative body for archivists and records managers working in the health sector, including but not limited to the NHS. Its membership is drawn from across the UK and the Republic of Ireland. It has been an affiliated group of the Society of Archivists'

Specialist Repositories Group since 2001. HARG aims to raise the profile of health archives and to improve the level of awareness in the NHS and elsewhere about record-keeping issues.

## **T**

### **Tracking**

Creating, capturing and maintaining information about the movement and use of records. (BS ISO 15489-1:2001(E))

### **Transfer Of Records**

Transfer (custody) – Change of custody, ownership and/or responsibility for records. (BS ISO 15489-1:2001(E))

Transfer (movement) – Moving records from one location to another. (BS ISO 15489-1:2001(E))

## **U - Z**

### **UK Information Commissioner (See Also Scottish Information Commissioner)**

The UK Information Commissioner enforces and oversees the Data Protection Act 1998 in the UK and Scotland, and liaises with the Scottish Information Commissioner with regards to the interaction between the Data Protection Act 1998 and the Freedom of Information (Scotland ) Act 2002.

### **Weeding**

The process of removing inactive/non-current records from the active/current or primary records storage area to a designated secondary storage area after a locally agreed timescale after the date of last entry in the record.

In an archiving sense, weeding can also mean the removal of records during appraisal which are not suitable for permanent retention and should be destroyed.

# **ANNEX B - RESOURCES TO SUPPORT IMPROVEMENT**

## **The Role of the Information Governance Framework and the Information Governance Toolkit**

Information Governance is defined as:-

“A framework for handling information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service”.

It is the information component of Clinical Governance and it aims to support the provision of high quality care to patients and clients and service users by promoting the effective and appropriate use of personal, sensitive information.

The Information Governance Framework enables NHS Boards and staff working within them, to ensure that personal information is dealt with legally, securely, effectively and efficiently. The focus is on setting standards and giving NHS Boards the tools to help them to incrementally achieve the defined requirements and make appropriate improvements to their service, which is sustained.

The Information Governance Framework addresses the following key areas when handling information:

- Caldicott recommendations on the use of patient identifiable information;
- NHS Scotland Confidentiality Code of Practice;
- Data Protection Act 1998;
- Freedom of Information (Scotland) Act 2002;
- Information Management and Technology Security (ISO 17799 Code of Practice for Information Security Management);
- Health and Corporate Records Management;
- Information Quality Assurance.

The Information Governance Framework also enables the NHS to monitor and manage change by educating staff, developing codes of practice, helping organisations and individuals to understand the requirements of law and ethics in respect of information handling and the consequent need for changes to systems and processes. Furthermore, it enables the NHS to work in

partnership with patients and clients by respecting their preferences and choices and addressing their concerns about the use of sensitive, personal information. The Information Governance Toolkit provides the means by which NHS Boards can assess their compliance against the national information governance standards. The standards can be viewed [here](#)

The Standards in the toolkit explain and expand upon those published in the NHS QIS Clinical Governance and Risk Management Standards, which were published in October 2005. For further information please [visit here](#)

The reports produced by the toolkit will be shared with NHS QIS as part of the Clinical Governance and Risk Managements Standards peer review visits.

The Department of Health has published 'Setting and Achieving the NHS Standards for Record Management – A Roadmap'. The roadmap applies to England only, but may be of interest to a Scottish audience as it contains a range of practical tools and guidance, including a knowledge base and templates that have been designed to support organisations in the implementation of the principles contained in the English version of the NHS Records Management Code of Practice.

The content of the Roadmap will be reviewed and updated at regular intervals. The Roadmap is available electronically to all organisations [here](#)

## **Other Reference Material**

### **Good Practice Guidelines for General Practice Electronic Patient Records**

'SCIMP Good Practice Guidelines for General Practice Electronic Patient Records' for Scottish guidance on the transfer of electronic health records.

### **Quality and Outcomes Framework (QOF)**

The Primary Medical Services (Scotland) Act 2004 introduced the concept of the Quality and Outcomes Framework (QOF) as a voluntary contractual requirement for participating GP practices. The QOF provides a significant financial incentive to demonstrate achievement against a wide range of clinical and organisational quality standards.

### **Confidentiality and Disclosure of Information: General Medical Services**

The Scottish Guidance NHS Circular: PCA(M)(2005)10 'Confidentiality and Disclosure of Information: General Medical Services (GMS), Section 17c Agreements, and Health Board Primary Medical Services (HBPMS) Code of Practice and Directions' sets out guidance on the confidentiality of information held by contractors - referred to collectively in this document as "contractors" – who provide General Medical Services (GMS), Section 17C Agreements and Health Board Primary Medical Services (HBPMS). Find out more [here](#)

### **Code of Practice on Records Management - Section 61 of Freedom of Information (Scotland) Act**

The Scottish Ministers 'Code of Practice on Records Management' under Section 61 of the Freedom of Information (Scotland) Act 2002. Find out more [here](#)

The Code of Practice provides guidance to all public authorities as to the practice which it would, in the opinion of the Scottish ministers, be desirable for them to follow in connection with the management of records under the Freedom of Information (Scotland) Act 2002.

### **Records Management: NHS Code of Practice (Department of Health)**

The Records Management: NHS Code of Practice, on which this guidance is based, was published by the Department of Health as guidance to NHS organisations in England on 30 March 2006. Find it [here](#)

### **The National Archives of Scotland: Model Action Plan for Developing Records Management**

The National Archives of Scotland: Model Action Plan for Developing Records Management Arrangements Compliant with the Code of Practice on Records Management under Section 61 of the Freedom of Information (Scotland) Act 2002 can be found [here](#)

A records management action plan detailing the steps that health service organisations should take to reach the standards set out in the Scottish Ministers' Code of Practice.

## **The National Archives of Scotland: Developing a Policy for Managing Email**

'The National Archives Guidelines on developing a policy for managing e-mail can be found [here](#)

## **The Royal College of Pathologists: The retention and storage of pathological records and specimens (4<sup>th</sup> edition, 2009 )**

The document contains guidance from The Royal College of Pathologists and the Institute of Biomedical Science regarding the management of pathology records.

## **Recommendations for the retention of pharmacy records (2008)**

Guidance on retention periods for pharmacy records can be obtained from the Royal Pharmaceutical Society.

## **Information Commissioner : CCTV Code of Practice**

The Code of Practice provides guidance and advice for CCTV users on how to comply with the Data Protection Act and also includes a simple checklist for users of very limited CCTV systems where the full provisions of the code would be too detailed.. This code is available [here](#)

## **Information Commissioner: The Use and Disclosure of Health Data**

Find this document [here](#)

Information Commissioner : How does the Data Protection Act Apply to Recording and Retaining Professional Opinions

This good practice note aims to inform organisations and practitioners about some of the data protection issues that arise in relation to the information about individuals that they record in their professional opinions [here](#)

## **Active Records Management: Records Creation**

A document that provides advice and guidance on the creation of paper-based files, it does not cover the creation of electronic files. It deals with the creation of registered files including policy, administrative and case files but not staff personal files. Find out more [here](#)

### **e-Government Technical Standards**

There are a number of Government standards which aim to ensure the consistency of electronic information transferred between public organisations or made available to the public through means such as websites. e-GIF is mandatory for all public sector bodies, including the NHS. Full details can be found [here](#)

### **Health and Social Care Data Standards**

The National Clinical Dataset Development Programme was established by the Chief Medical Officer in 2003 to support clinicians developing national clinical data standards, initially to support the national priority areas. These standards are an essential element of the Electronic Health Record, a central aim of the [National e-Health Strategy](#).

Further information can be obtained from their website [here](#) and the standards are published in the Health and Social Care Data Dictionary [here](#)

### **Health Rights Information Scotland (HRIS)**

HRIS provide clear accurate and up to date information about health rights. This includes information about what patients can expect from the NHS, accessing health records and being involved about decisions about their health care. Full details of publications can be found [here](#)

### **University of Edinburgh Records Management Section**

Access their site [here](#)

### **University of Edinburgh file naming conventions**

This document has been prepared as part of the Policy and Planning Records Management Project and is aimed primarily at people working within Academic Affairs, Planning and Secretariat departments in higher education. However, the principles will be beneficial to all staff working with corporate records including staff in NHS organisations. Find out more [here](#)

### **Scanning and Document Management in General Practice (May 2006)**

SCIMP have produced this simple [guide](#) to implementing the single scanning and document management system that has now been procured for Scottish General Practices.

## **Healthcare Information Governance Post-Graduate Education Programme**

Unit 2 focuses on [Records Management](#)

### **Information Governance in NHS Scotland: a competency framework**

Provides a foundation for the development, commissioning and review of information governance related education and training. The [Framework](#) is a set of national competencies describing what healthcare staff should know and be able to do in relation to information governance. The competences are arranged in five 'domains' (holding, obtaining, recording, using and sharing information) and four levels ('Foundation' to 'Advanced'). This approach will enable managers and training providers to tailor learning to the particular needs of staff groups.



## Useful Contacts

### Scottish NHS Archives and The National Archives of Scotland

There are at present three NHS archivists providing archive services to NHS Boards in Scotland. They can provide advice on the selection and preservation of healthcare records and the management of current records.

Mike Barfoot  
Lothian Health Services Archive  
Edinburgh University Library  
George Square  
Edinburgh  
EH8 9LJ  
Tel: 0131 650 3392  
E-mail: [lhsa@ed.ac.uk](mailto:lhsa@ed.ac.uk)

Alistair Tough  
Greater Glasgow and Clyde NHS Board Archive  
University of Glasgow Archives  
77-81 Dumbarton Road  
GLASGOW  
G11 6PW  
Tel: 0141 330 2992 or 0141 287 2883  
Fax: 0141 330 4158  
E-mail: [A.tough@Archives.gla.ac.uk](mailto:A.tough@Archives.gla.ac.uk)

Fiona Watson  
Northern Health Services Archives  
Victoria Pavilion  
Woolmanhill Hospital  
Aberdeen  
AB25 1LD  
Tel: 01224 555562  
E-mail: [f.watson@nhs.net](mailto:f.watson@nhs.net)

For advice on archiving in the NHS Tayside area contact:

Pat Whatley  
Archive, Records Management and Museum Services  
Tower Building  
University of Dundee  
DUNDEE  
DD1 4HN  
Tel: 01382 344095  
E-mail: [p.e.whatley@dundee.ac.uk](mailto:p.e.whatley@dundee.ac.uk)

Alternatively, the National Archives of Scotland (NAS) can provide advice about records management and archives. NAS does not offer an archive facility to local NHS boards and organisations, but can suggest appropriate archive contacts elsewhere:

National Archives of Scotland  
HM General Register House  
2 Princes Street  
EDINBURGH  
EH1 3YY  
Tel: 0131 535 1314  
E-mail: [enquiries@nas.gov.uk](mailto:enquiries@nas.gov.uk)

The National Archives of the United Kingdom(TNA) published a 'Code of Practice for Archivists and Records Managers under Section 51(4) of the Data Protection Act 1998' (Oct 2007). [Chapter 3](#) summarises the particular responsibilities of records managers in relation to personal data. Archival advice about moving images can be obtained from:

Scottish Screen Archive  
249 West George Street  
Glasgow  
G2 4QE  
Tel: 0845 300 7300

### **Scottish Government eHealth Directorate**

Scottish Government eHealth Directorate  
St Andrews House  
Regent Road  
EDINBURGH  
EH1 3XD  
Tel: 0141 242 0426  
E-mail: [robert.bryden@scotland.gsi.gov.uk](mailto:robert.bryden@scotland.gsi.gov.uk)  
Tel: 0131 244 2351  
E-mail: [kim.kingan@scotland.gsi.gov.uk](mailto:kim.kingan@scotland.gsi.gov.uk)

### **Information Commissioner – Scotland Office**

(Data Protection Act 1998)

93 - 95 Hanover Street  
Edinburgh  
EH2 1DJ  
Telephone: 0131 301 5071  
Email: [Scotland@ico.gsi.gov.uk](mailto:Scotland@ico.gsi.gov.uk)  
Website: <http://www.ico.gov.uk/>

## **Scottish Information Commissioner**

(Freedom of Information (Scotland) Act 2002)

Kinburn Castle  
Doubledykes Road  
St Andrews  
Fife  
KY16 9DS  
Tel: 01334 464610  
Fax: 01334 464611  
E-mail: [enquiries@itspublicknowledge.info](mailto:enquiries@itspublicknowledge.info)  
Website: [www.itspublicknowledge.info](http://www.itspublicknowledge.info)

## **NHSScotland Information Governance Programme**

Information Governance Team  
NHS National Services Scotland  
Gyle Square  
1 South Gyle Crescent  
EDINBURGH  
EH12 9EB  
Tel: 0131 275 7867  
Email: [NSS.infogov@nhs.net](mailto:NSS.infogov@nhs.net)  
Website: [www.elib.scot.nhs.uk/infogov](http://www.elib.scot.nhs.uk/infogov)

# ANNEX C: 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. Where necessary, organisations should obtain professional legal advice on the application of these provisions. A list of key legal and professional obligations covering personal and other information listed in this Annex is below:

## Legislation contents

1. [Anti-Terrorism, Crime and Security Act 2001](#)
2. [The Abortion \(Scotland\) Regulations 1991](#)
3. [The Access to Health Records Act 1990](#)
4. [The Access to Medical Reports Act 1988](#)
5. [The Census \(Confidentiality\) Act 1991](#)
6. [The Computer Misuse Act 1990](#)
7. [The Consumer Protection Act \(CPA\) 1987](#)
8. [The Control of Substances Hazardous to Health Regulations 2002](#)
9. [The Copyright, Designs and Patents Acts 1990](#)
10. [The Crime and Disorder Act 1998](#)
  - Section 115 relates to the disclosure of information
11. [The Data Protection Act \(DPA\) 1998](#)
  - The Data Protection (Processing of Sensitive Personal Data) Order 2000
12. [The Disability Discrimination Act 1995](#)
13. [The Electronic Communications Act 2000](#)
14. [The Environmental Information \(Scotland\) Regulations 2004](#)
15. [The Freedom of Information \(Scotland\) Act 2002 \(FOISA\)](#)
16. [The Gender Recognition \(Disclosure of Information\) \(Scotland\) Order 2005](#)
17. [The Health and Safety at Work Act 1974](#)
18. [The Human Fertilisation and Embryology Act 1990, as Amended by the Human Fertilisation and Embryology Act 2008](#)
19. [The Human Rights Act 1998](#)

20. [The Human Tissue \(Scotland\) Act 2006 – Part 1 Section 19 and Part 3 \(Maintenance of Records and Supply of Information Regarding the Removal and Use of Body Parts\) Regulations 2006 \(SSI 2006 No. 344\)](#)
21. [The Local Electoral Administration and Registration Services \(Scotland\) Act 2006](#)
22. [The Mental Health \(Care and Treatment\) \(Scotland\) Act 2003](#)
23. [The Prescription and Limitation \(Scotland\) Act 1973](#)
24. [The Privacy and Electronic Communications \(EC Directive\) Regulations 2003](#)
25. [Public Health Legislation in Scotland](#)
26. [The Public Interest Disclosure Act 1998](#)
27. [Public Records \(Scotland\) Act 1937](#)
28. [The Radioactive Substances Act 1993](#)
  - The High-activity Sealed Radioactive Sources and Orphan Sources Regulations
29. [The Re-use of Public Sector Information Regulations 2005](#)

## **Other Obligations contents**

30. [Administrative Law](#)
31. [The Blood Safety and Quality Regulations 2005](#)
  - Directive 2002/98/EC of the European Parliament and of the Council of 27 January 2003
  - Commission Directive 2005/61/EC of 30 September 2005
32. [The Common Law Duty of Confidentiality](#)
33. [NHS Scotland Code of Practice on Protecting Patient Confidentiality](#)
34. [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](#)

## **Relevant Standards and Guidelines contents**

1. BS ISO 15489-1: Designing and Implementing Records Keeping Systems – DIRKS
2. BSI PD 0016: 2001: Document Scanning. Guide to scanning business documents
3. BSI BIP 0008: Evidential Weight and Legal Admissibility of Information Transferred Electronically
4. BS 4783-8:1994: Storage, Transportation and Maintenance of Media for Use in Data Processing and Information Storage
5. BS 5454:2000: Recommendations for the Storage and Exhibition of Archival Documents
6. BS ISO/IEC 17799:2005 BS ISO/IEC 27001:2005 BS 7799-2:2005: Information Security Management
7. PD ISO/TR 15489-2:2001: Best Practice in Records Management
8. BS ISO 19005-1:2005: Document Management

## **Professional Codes of Conduct and Guidance**

35. The General Dental Council, Standards for Dental Professionals (06/05)
36. The General Medical Council: Good Medical Practice (2006)
37. Health Professionals Council: Standards for Conduct, Performance and Ethics (07/08)
38. The code: Standards of conduct, performance and ethics for nurses and midwives NMC (01/08)
39. Nursing and Midwifery Council, Record Keeping Guidance (07/09)
40. Nursing and Midwifery Council: Midwives Rules and Standards (05/04)
41. The Chartered Society of Physiotherapy: Rules of Professional Conduct (2005)
42. The Chartered Society of Physiotherapy: General Principles of Record Keeping and Access to Health Records (2000)
43. Scottish Social Services Council: Codes of Practice for Social Service Workers and Employers (2009)

## Legislation

**Note:** this section contains links to the 'OPSI' website. The opsi web version of legislation is as originally enacted, and does not include subsequent amendments. The links should therefore be treated with caution, and legal advice obtained when necessary.

### 1. Anti-Terrorism, Crime and Security Act 2001

Schedule 2 (part 3) covers disclosures on personal information in relation to suspected terrorists. See [here](#)

### 2. The Abortion (Scotland) Regulations 1991

The regulations set out the terms on which certificates of opinion must be issued and held by medical practitioners in order to comply with the Abortion Act 1967. The practitioner who carried out the termination must notify the Chief Medical Officer (CMO) of this fact within seven days of the termination. Under the regulations, these certificates must be retained by the practitioner who carried out the termination for a period of at least three years. Find out more [here](#)

#### **Records management considerations:**

To meet the requirements of these regulations, organisations must ensure that they have processes in place to ensure that certificates are retained in a secure area for at least three years, and that they are confidentially destroyed once they are no longer required.

### 3. The Access to Health Records Act 1990

Access to the health records of a deceased person is governed by the Access to Health Records Act 1990. It applies only to records created since 1 November 1991.

The Act allows access to:

- a) the deceased's personal representatives (both executors or administrators) to enable them to carry out their duties; and
- b) anyone who has a claim resulting from the death.

However, this is not a general right of access, it is a restricted right and the following circumstances could limit the applicant's access:

if there is evidence that the deceased did not wish for any or part of their information to be disclosed; or

- if disclosure of the information would cause serious harm to the physical or mental health of any person; or
- if disclosure would identify a third party (i.e. not the patient nor a healthcare professional) who has not consented to that disclosure.

As with the Data Protection Act, a medical professional may be required to screen the notes before release.

Under the Act, if the record has been updated during the 40 days preceding the access request, access must be given within 21 days of the request.

Where the record concerns information all of which was recorded more than 40 days before the application, access must be given within 40 days, however, as with the Data Protection Act 1998, organisations should endeavour to supply the information within 21 days.

### **FEE STRUCTURE**

The following maximum fees apply:

<b>Record Type</b>		<b>Fee</b>
<b>Viewings</b>	< 40 days	£0
	>40 days	£10
<b>Photocopies for Deceased patient records</b>	All	£10 admin fee + cost of making the copies @ 10p per sheet + p&p – to not exceed a maximum of £50

Health professionals may charge a professional fee to cover the costs of giving access to the records of deceased patients that is not covered by legislation.

**TIMING:** The information should be provided once the relevant information, including evidence of identity and fee has been received.

**PHOTOCOPYING CHARGES:** This will be charged at 10p per page of copy.



### **Records management considerations:**

Organisations should have processes that address where and how the records of deceased persons are stored. Secure and environmentally safe storage is vital to ensure that records are maintained in good order and are available if required. It is essential that organisations put in place processes and procedures to enable the efficient and effective retrieval of such records within the timescales specified by the Act.

#### **4. The Access to Medical Records Act 1988**

The aim of the Act is to allow individuals to see medical reports written about them, for employment or insurance purposes, by a doctor who they usually see in a 'normal' doctor/patient capacity. This right can be exercised either before or after the report is sent. The chief medical officer of the employer/insurer is the applicant and he/she will send a request for a report to the doctor. The request must be accompanied by a written and signed patient consent. The patient may view the report by obtaining a photocopy, or by attending the organisation to read the report without taking a copy away. The patient has a right to view the report from the time it is written and has a window to do so before the report is supplied, or he/she may view it after supply for up to six months.

However, in certain circumstances the patient may be prohibited from viewing all or part of the report if:

- in the opinion of the doctor, viewing the report may cause serious harm to the physical or mental health of the patient; or
- access to the report would disclose third-party information where that third party has not consented to the disclosure.

The patient retains the right to withdraw consent to the report's preparation and/or supply at any time. Therefore, if the patient is unable to view any of the report due to one of the circumstances listed above, he/she can refuse to allow it to be supplied. If a patient disagrees with the content of the report, he/she has several options. He/she can:

- a) refuse to allow its supply;
- b) ask the doctor to correct agreed inaccuracies; or
- c) have a note added addressing the point(s) of disagreement.

### **Records management considerations:**

It is important that these reports remain accessible to the patient for at least six months after they have been supplied to the employer or insurer. After six months, organisations should consider whether retention is necessary; however, if they do decide to retain the report it must be accessible should a subsequent subject access request be made. In some organisations it may be easier to hold the report as part of the health record. However private medical reports carried out on NHS patients, usually for legal cases, should not be filed in NHS records. Find out more [here](#)

### **5. The Census (Confidentiality) Act 1991**

The [Act](#) makes it a criminal offence to unlawfully disclose personal census information. If the Registrar-General or any person currently or previously employed or contracted to supply services to him, discloses such information they are committing an offence. If any person further discloses information knowingly acquired by unlawful disclosure, they are committing an offence.

The defences to a charge of unlawful disclosure are that at the time of the alleged offence the person believed:

- that he was acting with lawful authority; or
- that the information in question was not personal census information and that he had no reasonable cause to believe otherwise.

The penalties if convicted are:

- in the sheriff court, up to twelve months' imprisonment and/or a fine; or
- in the high court, two years' maximum imprisonment and/or a fine.

### **Records management considerations:**

Any staff that may use census information for their work must be instructed on the lawful way in which they may use it and the processes put in place to ensure that unlawful disclosure does not occur.

## **6. The Computer Misuse Act 1990**

The Act is relevant to electronic records in that it creates three offences of unlawfully gaining access to computer programmes.

The offences are:

- unauthorised access to computer material;
- unauthorised access with intent to commit or cause commission of further offences;
- unauthorised modification of computer material.

Access is defined in the Act as:

altering or erasing the computer program or data;

copying or moving the program or data;

using the program or data; or

outputting the program or data from the computer in which it is held (whether by having it displayed or in any other manner).

Unlawful access is committed if the individual intentionally gains access; knowing he is not entitled to do so; and aware he does not have consent to gain access. The 'further offence' applies if unauthorised access is carried out with intent to commit or cause an offence. The 'modification' offence applies if an individual does any act causing unlawful modification of computer material and does so in the knowledge that such modification is unlawful, and with the intent to:

- impair the operation of any computer;
- prevent or hinder access to any program or data held in any computer; or
- impair the operation of any such program or the reliability of any such data.

### **Records management considerations:**

It is important that all staff members are aware of and comply with all security measures put in place to protect all health records. The organisation should have policies and procedures in place to facilitate compliance alongside disciplinary measures for failure to comply.

See [here](#) (section 13 covers proceedings in Scotland)

## **7. The Consumer Protection Act (CPA) 1987**

The [Act](#) was modified slightly for Scotland under The Consumer Protection Act 1987 (Product Liability) (Modification) (Scotland) Order 2001:

The Act allows persons who have suffered damage/injury to themselves or to their private property to make a compensation claim against the manufacturer or supplier of a product. The claimant does not need to prove that the manufacturer/supplier was negligent; merely that it was the product that caused the damage. An obligation for liability lasts for 10 years.

The general limitation period in respect of personal injury actions under the Prescription and Limitation (Scotland) Act 1973 is:

- three years from the date on which the cause of action accrued –effectively, the date the accident took place; or
- three years from the date of knowledge that a cause of action had accrued. When a person dies, the limitation period runs from:
  - three years from the date of death; or
  - three years from the date when the personal representative had knowledge that a cause of action had accrued – i.e. the date when they realised that someone was potentially liable for the death.

### **Records management considerations :**

The NHS is affected by these provisions and may be liable as a supplier or user of a product. Therefore, it is important that accurate records are maintained for all products that may fall into this category in order that any claim can be defended

## **8. The Control of Substances Hazardous to Health Regulations (COSHH) 2002**

The [COSHH regulations](#) specify the eight measures that employers must follow to prevent or limit their employees' exposure to hazardous substances.

The measures are:

- assess the risks;
- decide what precautions are needed;
- prevent or adequately control exposure;
- ensure that control measures are used and maintained;

- monitor the exposure;
- carry out appropriate health surveillance;
- prepare plans and procedures to deal with accidents, incidents and emergencies;
- ensure employees are properly informed, trained and supervised.

**Records management considerations:**

The regulations require that organisations retain records of risk assessments, control measures, exposure monitoring and health surveillance. Some of these records must be kept for specified periods; these are detailed in the retention schedule at Annex [D](#) and [E](#).

**9. The Copyright, Designs and Patents Act 1988**

The Act protects the intellectual property of individuals and requires that permission of the owner of the intellectual property is sought before any use of it is made – this includes storage and display on the NHS net and internet or other electronic information services. Organisation web pages should not contain, or distribute, text or images to which a third party holds an intellectual property right, without the express written permission of the author. The author may have quoted other people’s material and if this is the case, such a third party would also need to give permission.

**Records management considerations:**

Corporate web pages where information is published should be checked for infringement of the Act and/or that necessary permissions or acknowledgements have been given. If there is any doubt, check with your legal advisers.

**10. The Crime and Disorder Act 1998**

The Act provides for anti-social behaviour orders to be applied for by a police authority or a local authority against an individual aged 10 years and over.

**[The Anti-Social Behaviour Act \(2003\)](#)**

amends the 1998 Act, but Part 5 (misuse of air weapons) and Part 10 (general provisions) are the only parts of the act which extend to Scotland.

### **Records management considerations:**

Any request for disclosure under this Act must be referred to the Caldicott Guardian and possibly the organisation's legal advisors, who should decide whether such disclosure is necessary or proportionate.

See [here](#) (chapter II of Part I and chapter II of Part IV) are specific to Scotland).

### **11. The Data Protection Act (DPA) 1998**

The [Act](#) regulates the processing of personal data, held manually and on computer. It applies to personal information generally, not just to health records, therefore the same principles apply to records of employees held by employers, for example in finance, personnel and occupational health departments.

**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. It therefore includes such items of information as an individual's name, address, age, race, religion, gender, and physical, mental or sexual health.

**Sensitive Personal data** is defined as personal information consisting of information as to:

- a) the racial or ethnic origin of the data subject;
- b) his political opinions;
- c) his religious beliefs or other beliefs of a similar nature;
- d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- e) his physical or mental health or condition;
- f) his sexual life;
- g) the commission or alleged commission by him of any offence; or
- h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

In order to lawfully process sensitive personal data one of 19 conditions must be met. These are set out in schedule 3 of the Data Protection Act and include:

- explicit consent of the data subject;
- legal advice and establishing or defending legal rights;
- religion and health data for equality of treatment monitoring;
- detection of unlawful activity;
- records on racial equality.

**Processing** includes everything done with that information, i.e. holding, obtaining, recording, using, disclosure and sharing it. Using includes disposal, i.e. closure of the record, transfer to an archive or destruction of the record.

The Act contains three key strands. These deal with:

- notification by a data controller to the Information Commissioner;
- compliance with the eight data protection principles; and
- observing the rights of data subjects.

### **Notification by a data controller**

The data controller is the person who determines how and why personal information is processed. In practice, for NHS organisations the Health Board or practice is the data controller. This means that ultimate responsibility for notification will usually rest with the Chief Executive or GP. The action of notification can be delegated to the most appropriate person within the organisation, for example the Head of Information Management, or the Information Governance Lead. Notification is the process of informing the Information Commissioner of the fact that processing of personal data is being carried out within a particular organisation. Its purpose is to achieve openness and transparency – notification entries are placed in a register so that members of the public can check the type of processing being carried out by a particular organisation. The notification process involves completion of a form stating the name of the data controller and detailing the types of processing being carried out.

Notification can be done in one of three ways:

1. By completing the online form [here](#) then printing it and posting to the Information Commissioner;
2. By requesting a notification form [here](#)
3. By phoning the notification helpline on 01625 545 740

## **Code of Practice for Archivists and Records Managers under Section 51(4) of the Data Protection Act 1998**

The National Archives of the United Kingdom, the Society of Archivists, the Records Management Society and the National Association for Information Management published a 'Code of Practice for Archivists and Records Managers under Section 51(4) of the Data Protection Act 1998' in October 2007. [Chapter 3](#) summarises the particular responsibilities of records managers in relation to personal data.

### **Compliance with the eight data protection principles**

The eight principles advocate fairness and openness in the processing of personal information. The principles state that:

1. personal data shall be processed fairly and lawfully and must be processed in accordance with at least one of the conditions in schedule 2 of the Act. Where the data being processed is sensitive personal information (such as data relating to the physical or mental health of an individual), it must also be processed in accordance with at least one of the conditions in schedule 3 of the Act;
2. personal data shall be obtained only for one or more specified and lawful purpose;
3. personal data shall be adequate, relevant and not excessive for its purpose(s);
4. personal data shall be accurate and where necessary kept up to date;
5. personal data shall not be kept for longer than is necessary for its purpose(s);
6. personal data shall be processed in accordance with the rights of data subjects under this Act;
7. appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
8. personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.



## **Records management considerations:**

### Principle 1

The aim of this principle is to ensure that personal data are processed fairly and lawfully and in accordance with a relevant condition from the schedules to the Act.

To meet the fair processing requirement, individuals must be informed of the fact of processing, including what information will be collected, and how it will be held, recorded, used and shared.

The Information Commissioner has issued guidance about the meaning of fair processing which indicates that the processing of personal data for purposes other than those for which the data has been provided may be unfair.

To meet the lawful processing requirement, personal data must be processed in accordance with all relevant laws, that is, other statutes such as Article 8 of the European Convention on Human Rights or the common law, such as the duty of confidence.

Health records contain both personal and sensitive data within the terms of the Act, therefore processing can only be carried out if a condition from both schedules 2 and 3 is met.

The relevant condition to be satisfied for schedule 2 is likely to be one of the following:

- where the processing is necessary for the exercise of any functions conferred on any person by or under any enactment;
- where the processing is necessary for the exercise of any other functions of a public nature exercised in the public by any person;
- where the processing is necessary to protect the vital interests of the patient, ie a 'life or death' situation; or
- with the consent of the patient.

The relevant condition to be satisfied for schedule 3 is likely to be one of the following:

- for medical purposes by a health professional or by a person who owes the same duty of confidentiality as a health professional;

- where the processing is necessary to protect the vital interests of the patient or another person, i.e. a 'life or death' situation, where consent cannot be obtained or the data controller cannot reasonably be expected to obtain consent;
- where the processing is necessary to protect another person, where consent of the patient has been unreasonably withheld; or
- with the explicit consent of the patient.

Although the Act does not state that explicit consent is required for the processing of health information, compliance with the 'lawful' requirement means that the common law duty of confidence must be taken into account. This duty requires that information given in confidence may not be disclosed without the consent of the giver of that information. Therefore, where health information will be disclosed to someone outside the care team, consent to the processing is necessary – see Common Law Duty of Confidentiality.

### Principle 2

This principle requires that personal data is not processed in a way that is incompatible with the purpose for which it was obtained. Organisations need to specify how they process information in their notification to the Information Commissioner. They are then required to ensure that all processing carried out is in accordance with those stated purposes. Patients should be fully informed about the reason that their information is required, ie they are not misled into providing information for purposes of which they have no knowledge. If information is obtained for a specific purpose, it must not be used for anything else unless consent is obtained for further uses of the information. For example, identifiable patient information gathered to provide healthcare cannot be used for research unless patient consent is obtained or the information is anonymised. Similarly, employee information collected to enable salary payment should not be used for purposes unrelated to this, for example marketing of products and services, unless consent is obtained. This principle reinforces the first principle in that it enables patients and the public to find out how a particular organisation states it will use their information.

### Principle 3

The aim of this principle is to ensure that organisational records management policies and procedures are in place to support the gathering of relevant, adequate information that is not excessive for its purpose. Organisations should therefore ensure that the information collection procedures in place enable relevant questions to be asked and that training on information collection is made available to all relevant employees. Systems and processes should be designed to ensure only relevant information is captured and processed. The organisation should have procedures in place setting out 'need to know' access controls alongside processes that enable conformance to those controls for each member of staff.

### Principle 4

To ensure good data quality organisations should follow all the procedures and processes described in the Information Quality Assurance requirements of the Information Governance Toolkit [here](#) The requirements describe the procedures and processes that organisations should put in place to ensure that information is accurate and kept up to date.

### Principle 5

The organisation should have procedures and processes in place for records appraisal so that records are kept for no longer than necessary for the purpose for which they are processed. However, organisations should ensure that records are retained for the minimum periods specified in this Code.

The organisation should put in place arrangements for the closure and disposal (whether destruction or archiving) of records, and secure procedures to prevent unnecessary copying of information. Section 33 and schedule 8 part IV of the Act specifically provide that personal data can be retained for 30 years (or longer) for historical and research purposes. This is reinforced by the further detail given in the Data Protection (Processing of Sensitive Personal Data) Order 2000. GPs currently have an exemption under the Act from having to delete the records of patients no longer registered. This was negotiated by the Joint GP IT Committee to maintain the integrity of clinical system audit trails, whilst they are not transferable between clinical systems.

### Principle 6

See Rights of the Individual (below).

### Principle 7

Records storage conditions must provide environmentally safe protection for current and archived records.

Records must be protected by effective information security management and records management staff members should be aware of and comply with measures put in place. In the guidance issued by the Information Commissioner, certified compliance with ISO 7799–2005 is cited as one of the obvious ways of demonstrating conformance.

### Principle 8

This principle is not infringed if the explicit informed consent of the individual is obtained for the transfer. However organisations must ensure that their contract includes terms to cover the protection of the data by the agency to the equivalent of the protection provided by the Data Protection Act 1998.

### **Rights of the individual**

The Data Protection Act gives an individual several rights in relation to the information held about him/ her. This includes:

- The right of individuals to seek access to their records held by the health provider.
- Access covers the right to obtain a copy of the record in permanent form, unless the supply of a copy would involve disproportionate effort or the individual agrees that his/her access rights can be met some other way, for example by viewing the record.

Access must be given promptly and in any event within 40 days of receipt of the fee and request. If the application does not include sufficient details to identify the person making the request or to locate the information, those details should be sought promptly and the 40-day period begins when the details have been supplied.

However, the Secretary of State has issued guidance stating that healthcare organisations should endeavour to meet such requests within a 21-day

timescale. This is so that Data Protection Act access rights reflect the previous rights contained within the Access to Health Records Act 1990.

If access has been given, there is no obligation to give access again until a reasonable period has elapsed. What is reasonable depends on the nature of the data, the purposes for which it is processed and the frequency with which it has been altered.

The right of access is exercisable by the individual:

- making a written application to the organisation holding the records;
- providing such further information as the organisation may require to sufficiently identify the individual; and
- paying the relevant fee.

The fee for providing the individual with a copy of a computerised record is £10. For healthcare records held partially or entirely on paper, the maximum amount that can be charged is £50.

#### **DEFINITION OF A HEALTH RECORD:**

A “health record” is defined as being any record which consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual.

A “health record” can be held electronically or on paper or mix of both, including X-rays, MRI scan, videos or tape recordings. This means that whenever a subject access request is made, the information contained in such material must be supplied to the applicant within the fee structure described below:

#### **FEE STRUCTURE:**

<b>Record Type</b>		<b>Max Fee</b>
<b>View Only</b>	< 40 days	£0
	>40 days	£10
<b>All Electronic</b>	All	£10
<b>Part Electronic and other media</b>	Core Notes inc X-Rays	£50
<b>All paper</b>	Core Notes inc X-Rays	£50

If a patient wishes to view their records and subsequently makes a request for copies, the patient will be charged as per one access request, to a maximum of £50. The fees should be paid in advance. The above are the maximum fees, and cover all costs associated with labour, copying, postage or other forms of delivery.

Value Added Tax (VAT) should not be charged on the fee charged for responding to a subject access request.

There are two main exemptions from the requirement to provide access to personal data in response to a subject access request. These are:

- if the record contains third-party information (i.e. not about the patient or the treating clinician) where that third party is not a healthcare professional and has not consented to their information being disclosed. If possible, the individual should be provided with access to the part of the record that does not contain the third-party identifier;
- if 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.

#### **Records management considerations:**

Records management staff members have a key role in ensuring that health records can be located, retrieved and supplied in a timely manner. It is important that document management structures are set up in such a way as to enable them to carry out this role.

NHS Board record keeping policies include processes for ensuring that any changes or revisions made to patients written notes are reflected in any subsequent records systems manual or electronic. Whenever a change is considered significant the responsible recipient record holder should be informed in order that corrective action can be taken.

#### **The Data Protection (Processing of Sensitive Personal Data) Order 2000**

This Order amends the DPA 1998 and provides that sensitive personal data (for example information relating to physical or mental health) may be lawfully processed without explicit consent where there is a substantial public interest in disclosing the data for any of the following purposes:

- for the detection and prevention of crime;
- for the protection of members of the public against malpractice, incompetence,
- mismanagement etc;
- to publicise the fact of malpractice, incompetence, mismanagement etc, for the protection of the public;
- to provide confidential counselling and advice where explicit consent cannot be given nor reasonably obtained, or where the processing must be carried out without explicit consent so as not to prejudice that confidential counselling or advice; or
- to undertake research that does not support measures or decisions with respect to any particular data subject unless the data subject has explicitly consented and does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person Sensitive personal data may also be lawfully processed where: the information relates to the data subject or to specific relatives of the data subject and the processing is for the purposes of administering defined insurance business or occupational pensions schemes;
- the processing is carried out by a person authorised under the Registration of Political Parties Act 1998 in the course of their legitimate political business as long as the processing does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person; or
- the processing is necessary for the exercise of any functions conferred on a constable by any rule of law. Find out more [here](#)

## **12. The Disability Discrimination Act 1995**

Providers of goods and services must not treat a person with a disability less favourably than a person to whom such a disability does not apply. One practical interpretation is that where, because of a disability, a data subject is unable to complete a written subject access request, their request should be handled in a way that enables them to enjoy their right of subject access in a similar way to those who do not have a disability preventing them from submitting a request in writing. Find out more [here](#)

### **13. The Electronic Communications Act 2000**

The purpose of the Act is to increase confidence in electronic transactions by providing:

- legal admissibility for digital signatures;
- registration of cryptography services providers; and
- repeal of and amendments to legislation that places limits on electronic communication and electronic storage of information.

The Act refers to cryptographic service providers who may employ Public Key Infrastructure (PKI) technology. This technology can be used to limit access to information to those authorised to access it (via a private key), provide a legal basis for the use of digital signatures to verify the identity of the sender and/or to authenticate digital access credentials.

#### **Records management considerations:**

Organisations should ensure that electronic information is held and transferred in accordance with the Act and other provisions to ensure that confidential information is accessed only by those with a need to know it in order to carry out their role.

Organisations should be aware of the need to ensure the retention and protection of any cryptographic keys that have been used to protect records, as they may have evidential value over the lifetime of the record. Find out more [here](#)

### **14. The Environmental Information (Scotland) Regulations 2004**

The Environmental Information Regulations 2004 came into force on 1 January 2005 and update and extend previous rights to environmental information.

Any request for information held by/on behalf of a public authority is initially treated as a Freedom of Information request. However, section 39 of the Freedom of Information (Scotland) Act 2002 exempts environmental information from being dealt with under freedom of information and provides for it to be dealt with under the Environment Information (Scotland) Regulations (EIR) 2004. This means that there may be cases where information is exempt under freedom of information but has to be released



under these regulations. (Where there is a conflict between EU regulation and UK legislation, the EU law takes precedence.)

The regulations are very similar to the Freedom of Information (Scotland) Act 2002 and requests for environmental information are dealt with in a similar way to those for other information.

The key differences between EIR and the Freedom of Information Act are:

- a wider range of organisations are covered by the EIR, including some private organisations;
- the EIR relates to environmental information only;
- requests for information do not have to be in writing under the EIR; they can be verbal;
- EIRs have exceptions rather than exemptions and all of these are subject to the public interest test;
- the 20 day time period for responding to requests can be extended to 40 days where the request is complex and voluminous and would involve a considerable amount of work;
- provision for charging of fees is different – there is no upper or lower threshold and authorities can recover, in full, the cost of supplying the information;
- information relating to emissions has special status and will have to be supplied in most cases.

Find out more [here](#)

A comparative guide to dealing with requests under the Freedom of Information (Scotland) Act and the Environmental Information Regulations is available on the Scottish Information Commissioners website [here](#)

Personal information of the applicant continues to be dealt with under data protection.

### **Records management considerations:**

As with the Freedom of Information (Scotland) Act 2002 the organisation needs a robust records management programme. The requirements of the two pieces of legislation are similar so it is advised that organisations deal with

requests in a like manner. The main difference is that requests for environmental information need not be in writing.

### **15. The Freedom of Information (Scotland) Act 2002 (FOISA)**

The FOISA provides the right to access the information that is held by Scottish public authorities and requires a commitment from public authorities to proactively publish information.

For further information, guidance and resources on FOISA see [here](#)

The new rights of access in the FOISA signal a new recognition of, and commitment to, the public interest in openness about government. They are additional to other access rights, such as access to personal information under the Data Protection Act 1998, and access to environmental information under the EIR 2004.

The main features of the Act are:

- a general right of access to recorded information held by public authorities, regardless of the age of the record/document;
- a duty on every public authority to adopt and maintain a publication scheme, which sets out what information will be made available and how it can be accessed; and
- the establishment of the Scottish Information Commissioner, whose role is to promote and to enforce FOISA.

Section 61 of the Act places a duty on Scottish Ministers to issue a Code of Practice on records management. Although compliance with the Code is not obligatory, it provides guidance to all public authorities as to the practice which it would, in the opinion of Scottish Ministers, be desirable for them to follow in connection with the discharge of their functions under the FOI(S)A.

Additionally, the Code may be used by the Information Commissioner when deciding whether a public authority has properly dealt with a case (in the event of a complaint).

#### **General right of access**

The Act provides a general right of access to all information held by Scottish public authorities.

However, the Act recognises that there can be valid grounds for withholding information and provides a number of exemptions from the right to know, some of which are absolute exemptions and some of which are subject to a public interest test.

As regards exemptions subject to the public interest test, organisations must weigh up whether the public interest in maintaining the exemption in question outweighs the public interest in disclosure.

The request for information must:

- be in writing or other permanently recorded format;
- state the name of the applicant and an address for correspondence; and
- describe the information requested.

The applicant can request that information be communicated by:

- a copy in permanent form (or other form acceptable to them, for example on CD-ROM or audio tape);
- inspection of records; or
- a summary or digest of the information held.

Public Authorities must comply to a request promptly; and in any event by not later the 20th working day following receipt of the request and/or the appropriate fee if required. A public authority need not comply with vexatious requests or repeated requests for information already supplied unless a reasonable period has elapsed between requests. A fee may be charged by the public authority to cover the costs of locating, retrieving and providing the information requested.

This may include:

- staff time, up to a maximum charge of £15 per hour;
- the cost of putting the information into the applicant's requested format, for example CD, or audio tape;
- photocopying and printing costs and;
- postage or other transmission costs.

Where it is estimated that the costs of responding to a request will exceed £600 (the 'upper cost limit') a request for information may be refused. The first

£100 of costs may not be charged to the applicant, and thereafter a charge of 10% can be made. The maximum charge is therefore £50. Public authorities are not obliged to make a charge and in many cases may not find it practical to do so.

### **Publication scheme**

A publication scheme must be published by each public authority and approved by the Scottish Information Commissioner.

Publication Schemes must specify:

- the classes of information published, or intended to be published;
- the manner in which publication is, or is intended to be made;
- whether the information is available free of charge or whether payment is required.

### **Records management considerations:**

The organisation should carry out a records audit to determine what records it holds, the locations of the records and whether they need to be kept – this should lead to a review of the organisation's retention schedules and provide information for its publication scheme.

As with Data Protection Act subject access requests, records management staff and procedures are crucial to compliance with this Act. There is a duty imposed on organisations to supply information in a timely fashion – currently within 20 working days. To facilitate this obligation to provide information within these time limits the organisation must ensure that all employees are aware of how an FOISA application should be progressed and of the requirement to respond to requests quickly.

Organisations should consider maintaining a log of requests with the view to making frequently requested information available through its publication scheme.

## **16. The Gender Recognition Act 2004**

The Act gives transsexual people the legal right to live in their acquired gender. It established the Gender Recognition Panel, who have the authority to issue a Gender Recognition Certificate. Issue of a full certificate provides legal recognition of the transsexual person's acquired gender.

Under the Act, information relating to an application for a Gender Recognition Certificate is 'protected information' if it is acquired in a professional capacity. It is an offence to disclose protected information to any other person unless an exemption applies. Some of the exemptions are:

the person has consented;

- the person cannot be identified from the information;
- information is needed for prevention and investigation of crime;
- information is needed to comply with a court order.

See [here](#) (Part 2 of schedules 2, 3 and 4 are specific to Scotland)

Further information is available from the Department of Constitutional Affairs [here](#)

### **Records management considerations:**

Applicants to the Gender Recognition Panel are required to supply evidence from a medical practitioner in support of their application. As 'protected information' covers all information that would identify a person as being a transsexual, if successful in their application a new health record must be created so that protected information is not disclosed.

### **The Gender Recognition (Disclosure of Information) (Scotland) Order 2005**

It is not an offence to disclose the 'protected information' referred to under the Gender Recognition Act 2004 if:

- the disclosure is made for the purpose of obtaining legal advice;
- the disclosure is made in an official capacity in relation to an organised religion to disclose that information to any other person acting in such a capacity e.g. to enable a minister or religion to decide whether to solemnise or permit the marriage of the subject;
- the disclosure is made for medical purposes to a health professional; and the person making the disclosure reasonably believes that the subject has given consent to the disclosure or cannot give such consent;
- Specific disclosures in relation to credit reference agencies, insolvency and bankruptcy.

'Medical purposes' includes the purposes of preventative medicine, medical diagnosis and the provision of care and treatment. Find out more [here](#)

## **17. The Health and Safety at Work Act 1974**

The Act imposes duties on employers to look after the health and safety of their employees and responsibilities on employees to comply with the measures put in place for their health and safety.

There are also six regulations concerned with health and safety at work:

- Management of Health and Safety at Work Regulations 1999;
- Workplace (Health Safety and Welfare) Regulations 1992;
- Display Screen Equipment Regulations 1992;
- Provision and Use of Work Equipment Regulations 1992;
- Manual Handling Regulations 1992;
- Personal Protective Equipment Regulations 1992.

The regulations require that employers carry out risk assessments and provide employees with information and training where necessary.

The Management of Health and Safety at Work Regulations 1999 sets out more explicitly what organisations must do to comply with the Health and Safety at Work Act. The Health and Safety Executive has published an approved Code of Practice for use with the regulations, available [here](#)

The Code has a special legal status – a court will take account of whether an organisation has followed the Code in prosecutions for breach of health and safety legislation, unless the organisation can prove that they complied with the law in some other way.

### **Records management considerations:**

Organisations should retain equipment maintenance records, records of assessments and training records etc for appropriate periods, as proof that they are complying with the law and maintaining the safety of their employees. Retention of these records will also assist organisations to appropriately defend against any legal action and comply with investigations carried out by the Health and Safety Executive and/or the Healthcare Commission.

## **18. The Human Fertilisation and Embryology Act 1990 as amended by the Human Fertilisation and Embryology Act 2008**

The Act is retrospective and applies to information obtained before and after it was passed. The Act prohibits the disclosure by current and former members and employees of the Human Fertilisation and Embryology Authority of:

- any information contained within the Authority's register; and
- any information obtained with the expectation that it would be held in confidence.

The Human Fertilisation and Embryology Authority (Disclosure of Donor Information) Regulations 2004 (SI 1511) prescribe the information which the Authority will provide to persons who have attained the age of 18 and who may have been born in consequence of treatment services under the Act.

### **Records management considerations:**

To meet the requirements of this Act, organisations must ensure they have processes in place to ensure that such information is available only to those permitted access. This is especially important as regards paper records, where information on this form of treatment is likely to be included within past medical history (particularly hospital records). Find out more [here](#)

## **19. The Human Rights Act 1998**

The Act became part of UK law on 2 October 2000. It does not contain new rights. It incorporates the European Convention on Human Rights into UK law, allowing an individual to assert their Convention rights in UK courts and tribunals, rather than at the European Court in Strasbourg. The Act can be used only against a public body, therefore NHS and social care organisations, as public bodies, are subject to the Act. Article 8 of the Act – the right to respect for private and family life – is the most relevant to the health and social care setting.

**The Right to Respect for Private and Family Life** contains four rights.

These are:

- the right to respect for private life;
- the right to respect for family life;
- the right to respect for one's home; and
- the right to respect for correspondence.

Article 8 is not an absolute right, in that the Act makes provision for interference with the rights (see below). It does, however, impact on subject access requests, consent, confidentiality and disclosure issues.

### **The right to respect for private life**

The current approach is that the right to respect for private life includes an obligation on a public body to meet subject access requests. Denial of access could be interpreted as a breach of Article 8 as it prevents an individual gaining access to information held about him/her. This reflects the rights of the individual under the Data Protection Act 1998. Legislation must be read, as far as possible, in a way that is compatible with the Human Rights Act.

The right to respect for private life can also be invoked where treatment information is withheld from the individual. If an individual consents to treatment but has not been given sufficient information to make a fully informed decision that consent will not be valid. Arguably, the withholding of information is a breach of the Article 8 right.

The Article 8 right reflects the common law duty of confidentiality in that patient information should only be disclosed with that patient's consent. If information is inappropriately disclosed the individual can take legal action for breach against the public body concerned. Not only must patient information be held confidentially, it must also be held securely. Failure to do so will also breach the right to respect for private life.

### **The right to respect for family life**

This right may also be relevant, in that relatives of the ill often wish to be involved in the decision making process, and kept informed of progress. However, this right must be balanced against the patient's right to confidentiality.

The right to respect for family life becomes even more relevant where the patient is a child or 'incompetent' adult. Failure to keep the family informed can be seen as an interference with this right, actionable under the Act. However, in a situation where the child is 'competent' and does not wish for information to be shared with his/ her family, the young person's right to confidentiality is likely to outweigh the right of the family.



Explaining this may bring the professional into conflict with the family, but ultimately the right of the individual to have information held confidentially will outweigh the right of the family.

It may be possible to claim that one's rights in relation to respect for family life have been breached in an employment context. An employee under an excessive workload such that it impinges on his/her life outside of the work environment could possibly plead interference with his/her right to respect for family life.

### **The right to respect for correspondence**

Correspondence includes written and telephone communications. It may be relevant for an individual to assert this right in relation to the monitoring of workplace e-mails. In particular, if the employee has not been informed that he/she 'has no reasonable expectation of privacy' and that workplace monitoring is taking place. To lessen the risk of being sued under this heading an employer should ensure that:

- the organisation complies with the advice from the Information Commissioner;
- all employees are informed of the organisational policy on 'private' e-mails (which should also include the use of the telephone and the internet); and
- consistent decisions are taken if policy breaches are discovered.

### **Interference with an Article 8 right**

Article 8 rights are qualified rights; this means that in certain circumstances they can be set aside by the state. However, this interference must be lawful, for a legitimate social aim and necessary to achieve that aim. Furthermore, the interference must not be disproportionate to the objective to be achieved.

- Legitimate social aims are:
  - national security;
  - protection of public safety;
  - protection of health or morals;
  - prevention of crime or disorder;
  - protection of the economic well-being of the country; and
  - protection of the rights and freedoms of others.

The public body will have to weigh up the public interest necessity of breaching an Article 8 right against the rights of the individual.

**Records management considerations:**

Current understanding is that if organisations comply with the provisions of the common law duty of confidence and the Data Protection Act 1998 they will meet the requirements of Article 8. Find out more [here](#)

**20. The Human Tissue (Scotland) Act 2006 – Part 1 Section 19 and Part 3**

Deals with three distinct uses of human tissue. Also introduces the concept of Authorisation. Part 4 - defines 'nearest relative' and makes provision for witnessing of authorisations and related matters. Find out more [here](#)

**The Human Tissue (Scotland) Act 2006 (Maintenance of Records and Supply of Information Regarding the Removal of Body Parts Regulations.**

Requires those removing and receiving body parts to maintain records and supply information to NHSBT and relevant NHS Board. Find out more [here](#)  
20.1 The Human Tissue (Scotland) Act 2006 – A guide to its implications for NHS Scotland. HDL (2006) 46. Find out more [here](#)

**21. The Local Electoral Administration and Registration Services (Scotland) Act 2006**

The Local Electoral Administration and Registration Services (Scotland) Act 2006 (LEARS Act) introduced changes to the electoral system and registration service in Scotland. Under the Act the General Registrar Office for Scotland was given special powers to share information with other government departments, including the NHS. The Registrar General creates and maintains a register of individuals from the Register of Births and Deaths and the Adopted Children Register. See Section 57 of the Act for further information. Find out more [here](#)

## **22. The Mental Health (Care and Treatment) (Scotland) Act**

**2003**

The 2003 Act replaces the 1984 Act. It establishes new arrangements for the detention, care and treatment of persons who have a mental disorder. It also refines the role and functions of the Commission and establishes the Tribunal as the principal forum for approving and reviewing compulsory measures for the detention, care and treatment of mentally disordered persons. Part 18 makes miscellaneous provisions including the drawing up of a code of practice, the making of statements indicating a patient's wishes about treatment, the withholding of correspondence and communications from certain detained patients and the cross-border transfer of patients. Find out more [here](#)

## **23. The Prescription and Limitation (Scotland) Act 1973**

The [Act](#) sets out the law on the time limits within which actions for personal injuries, or arising from death, may be brought. The limitation period for bringing such actions is three years, based on the date on which the individual became aware of the damage.

Under the Prescription and Limitation (Scotland) Act 1973 a person who has been declared of unsound mind may sue for damages up to 3 years after being declared sound of mind. Unsoundness of mind does not mean insanity but an inability of the injured person by reason of their mental state to manage their own affairs in relation to the relevant event and injury. The provisions of the Act will not necessarily apply to all mental health records, but where an action is initiated it will affect not only the mental health records, but all the health records of that patient. For example, a patient on being declared sound of mind has 3 years in which to sue for damages in relation to a hip operation performed while he was unsound of mind even if that operation had been performed 20 years earlier.

### **Records management considerations:**

It is important that accurate records are retained in accordance with national guidance and local policies. As with other statutory provisions, organisations must be able to locate and supply the information if requested and ensure that closed records are stored in accordance with national guidance.

## **24. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (no. 2426) and The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2004 (no. 1039)**

These Regulations revoke the Telecommunications (Data Protection and Privacy) Regulations 1999 and are concerned with the processing of personal information and the protection of privacy in the electronic communications sector.

The Regulations set out:

- circumstances under which direct marketing may be carried out;
- duties to safeguard the security of a communications network service;
- limitations on what may be stored or accessed; and
- restrictions on the processing of traffic and location data.

The Regulations are enforced by the UK Information Commissioner. See links [here](#) and [here](#)

## **25. Public Health Legislation in Scotland**

The Public Health Scotland Act 2008 passed by the Scottish Parliament on 12th June 2008 and received Royal Assent on 16th July 2008

This Act restates and amends the law on public health; to make provision about mortuaries and the disposal of bodies; to enable the Scottish Ministers to implement their obligations under the International Health Regulations; to make provision relating to the use, sale or hire of sunbeds; to amend the law on statutory nuisances; and for connected purposes.

## **26. The Public Interest Disclosure Act 1998**

The [Act](#) allows a worker to breach his duty as regards confidentiality towards his employer for the purpose of 'whistle-blowing'. A disclosure qualifying for protection under the Act is known as a 'qualifying disclosure'.

Such a disclosure is allowed in the following circumstances:

- where criminal activity or breach of civil law has occurred, is occurring, or is likely to occur;
- where a miscarriage of justice has occurred, is occurring or is likely to occur;
- where health and safety has been, is, or is likely to be compromised;
- where the environment has been, is being or is likely to be damaged; or

- where information indicating evidence of one of the above circumstances is being or is likely to be deliberately concealed.

It makes no difference whether the circumstance leading to the breach is within or outside of the UK, as long as either UK law or the law of the other jurisdiction prohibits it.

A qualifying disclosure must only be made:

- in good faith to the individual's employer, or to any other person having legal responsibility for the conduct complained of;
- for the purpose of obtaining legal advice;
- where the worker is employed by the Crown, in good faith to a Minister the Crown; or
- in good faith to a person prescribed by the Secretary of State.

Under this Act, the worker must reasonably believe that any allegation he makes is substantially true.

If it is the employer who is responsible for the conduct complained of, the Act allows a worker to make a disclosure to a person not noted above, provided the following conditions are met:

- it must be made in good faith, and not for personal gain, with a reasonable belief that the allegations complained of are true; and
- the worker reasonably believes he will suffer a detriment if he makes the disclosure to his employer; or
- he has previously complained of the conduct and no action has been taken; or
- he reasonably believes that evidence of the conduct has been or will be destroyed or concealed.

Such a disclosure will be subject to a test of reasonableness, which is tested with reference to:

- the person the disclosure was made to;
- the seriousness of the conduct complained of;
- whether the conduct is continuing;
- whether any previously made complaint was acted upon; and
- whether the worker followed any procedure laid down by the employer.

### **Records management considerations:**

Staff should be made aware of the correct procedures to be followed if circumstances arise that require them to breach confidentiality and any policy guidance/Health Service Circular on 'Public Interest Disclosure' available on the issue.

### **27. The Public Records (Scotland) Act 1937**

Find out more [here](#)

### **28. The Radioactive Substances Act 1993**

Find out more [here](#)

### **The High-activity Sealed Radioactive Sources and Orphan Sources Regulations**

The Act applies to organisations that keep, use or dispose of radioactive material or waste. It is supplemented by the High-activity Sealed Radioactive Sources and Orphan Sources Regulations (HASS), which applies additional requirements on organisations that use or dispose of sealed radioactive sources, for example those used for radiography and radiotherapy.

Organisations who keep or use radioactive material or sources must obtain a certificate of registration from the Environment Agency, whilst those who dispose of radioactive waste or sources must obtain a certificate of authorisation. Find out more [here](#)

### **Records management considerations:**

Records relating to radioactive substances and radioactive waste must be retained as specified by the Environment Agency. The Agency may also require that records be retained for a specified period after the activity has ceased. Once this period has expired, records should be filed with an appropriate repository, ie a Place of Deposit.

## **29. The Re-use of Public Sector Information Regulations 2005**

The Regulations link with the Freedom of Information (Scotland) Act 2002, in that freedom of information is about access to information and these regulations are about how the information can be re-used. However, there is no automatic right to re-use merely because an access request has been granted. Information that is exempt under FOISA or other legislation is also exempt under the Regulations.

Health Service bodies are required to:

- publish the terms and conditions of standard licences for re-use;
- compile an information asset register detailing the information available for re-use;
- publish details of any exclusive re-use licences granted and review those licences every three years;
- notify the applicant of the reasons for refusal of a re-use application;
- provide contact details where complaints can be addressed;
- deal with all applicants in a non-discriminatory manner, for example applying the same charges for the same type of use; and respond to requests within 20 working days.

### **Records management considerations:**

Employees responsible for re-use issues should work closely with those responsible for FOI for several reasons. These include:

- an information audit is required for both pieces of legislation to determine the records held and the locations of those records;
- information available for re-use and the terms and conditions of re-use can be included within the organisation's publication scheme (see Freedom of Information (Scotland) Act 2002); and
- if a request is made for access and re-use, the processes need to be coordinated so that the access issue is dealt with before permission to re-use is granted.

## Other obligations

### 30. Administrative Law

Administrative law governs the actions of public authorities. According to well-established rules, a public authority must possess the power to carry out what it intends to do. It is also necessary that the power is exercised for the purpose for which it was created or is 'reasonably incidental' to the defined purpose. If not, its action is 'ultra vires' i.e. beyond its lawful powers. It is important that all NHS bodies are aware of the extent and limitations of their powers and act 'intra vires'. The approach often adopted by Government to address situations where a disclosure of information is prevented by lack of function (the 'ultra vires' rule), is to create, through legislation, new statutory gateways that provide public sector bodies with the appropriate information disclosure function. However, unless such legislation explicitly requires that confidential patient information be disclosed, or provides for common law confidentiality obligations to be set aside, then these obligations must be satisfied prior to information disclosure and use taking place, for example by obtaining explicit patient consent.

#### **Records management considerations:**

Staff should be trained in the legal framework covering the disclosure of confidential patient information. They should also be provided with procedures for obtaining explicit consent and guidance on where to seek advice if they are unsure whether they should disclose such information. Find out more [here](#)

### 31. Blood Safety and Quality Legislation

The Blood Safety and Quality Regulations 2005 (amended by the Blood Safety and Quality and Quality (Amendment) (No. 2) Regulations 2005)

The regulations implement the provisions of Directive 2002/98/EC (below) so that the retention periods for data relating to human blood and blood components outlined in the Directive are now part of UK law.

The retention periods are as follows:

- blood establishments must retain certain information regarding donors, establishment



- activity and testing of donated blood for a minimum of 15 years (regulation 7);
- blood establishments and hospital blood banks must retain data needed for full traceability for at least 30 years from the point of receipt of the blood or blood component (regulations 8 and 9).

The regulations also set out requirements for maintaining the confidentiality and security of data (regulation 14) and provide that identifiable information held by blood establishments and blood banks must not be disclosed to third parties unless it is for one of the following reasons:

- to comply with a court order;
- to assist an inspector appointed by the Secretary of State in accordance with these regulations; or
- to enable tracing of a donation from donor to recipient or from recipient to donor.

Find out more [here](#)

#### **Records management considerations:**

Organisations must ensure that they are able to provide full traceability of whole blood and blood components. There should be a record keeping system that:

- allows for identification of each single blood donation and each single blood unit and components thereof; and
- enables full traceability to the donor as well as to the transfusion and the recipient. That is, the method of recording must unmistakably identify each unique donation and type of blood component, the location at which the donation was received and to whom that donation was given.

#### **Directive 2002/98/EC of the European Parliament and of the Council of 27 January 2003**

The directive sets standards of quality and safety for the collection and testing of human blood and blood components, whatever their intended purpose, and to their processing, storage, and distribution when intended for transfusion.

Find out more [here](#)

### **Commission Directive 2005/61/EC of 30 September 2005**

The annexes of this directive set out the data that should be retained for 30 years in order to comply with the traceability requirements of Directive 2002/98/EC.

- Data to be retained by blood establishments:
- blood establishment identification;
- blood donor identification;
- blood unit identification;
- individual blood component identification;
- date of collection (year/month/day); and
- facilities to which blood units or blood components are distributed, or subsequent disposal.

#### **Data to be retained by hospital blood banks:**

- blood component supplier identification;
- issued blood component identification;
- transfused recipient identification;
- for blood units not transfused, confirmation of subsequent disposal;
- date of transfusion or disposal (year/month/day); and lot number of the component, if relevant.

### **32. The Common Law Duty of Confidentiality**

Common law is not written out in one document like an Act of Parliament. It is a form of law based on central principles and the decisions of judges in previous court cases. The law is applied by reference to those previous cases, so common law is also said to be based on precedent.

The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

In practice, this means that all patient information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient. It is irrelevant how old the patient is or what the state of their mental health is; the duty still applies.

Three circumstances making disclosure of confidential information lawful are:

- where the individual to whom the information relates has consented;
- where disclosure is in the public interest; and
- where there is a legal duty to do so, for example a court order.

Therefore, under the common law, a healthcare provider wishing to disclose a patient's personal information to anyone outside the team providing care should first seek the consent of that patient.

Where this is not possible, an organisation may be able to rely on disclosure being in the overriding public interest. However, claiming a disclosure is in the public interest should not be done lightly. Solid justification is required before individual rights are set aside and specialist or legal advice should be sought before the information is disclosed. Any decision to disclose should be fully documented. It will ultimately be up to a court to decide whether the public interest justification is sufficient.

Disclosures required by court order should be referred to the organisation's legal advisors as promptly as possible, so that any necessary representations may be made to the court, for example to limit the information requested.

If a disclosure is made which is not permitted under common law the patient may be able to bring a legal action not only against the organisation but also against the individual responsible for the breach.

### **Records management considerations:**

All persons involved in the records management function should be aware of their responsibility for maintaining confidentiality of records. Employees should only have access to those parts of the record required to carry out their role. Requests for records access by other staff members should be logged and periodically audited. Particular care should be taken during the transportation of health records outside of the organisational site, for example security envelopes and approved carriers should be used where necessary.

### **33. NHS Scotland Code of Practice on Protecting Patient Confidentiality**

The Code offers detailed guidance on:

- protecting confidential information;
- informing patients about uses of their personal information;

- offering patients appropriate choices about the uses of their personal information; and
- the circumstances in which confidential information may be used or disclosed.

The Code can be accessed from the Information Governance e-Library website in 'The Basics' section.

#### **Disclosure after a patient's death:**

Although there are no legal obligations of confidentiality that apply to the deceased, the ethical obligation to respect a patient's confidentiality extends beyond death. The duty of confidentiality needs to be balanced with other considerations, such as:

- to assist a Procurator Fiscal or other similar officer in connection with an inquest or fatal accident inquiry;
- as part of national confidential enquiries; or
- on death certificates;
- where a person has a right of access under the Access to Health Records Act 1990; and
- those close to the deceased.

Deceased patient records are fully accessible after a period of one hundred years from the beginning of the calendar year following the date of last entry under the Freedom of Information (Scotland) Act 2002.

#### **34. 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**

The directive lays down rules governing the production, distribution and use of medicinal products. It is relevant here as it sets retention periods for information gathered in the course of clinical trials.

The trial investigator has a duty to retain patient identification codes for at least 15 years following the trial.

The health organisation at which the trial was carried out must retain the health records of the patients involved for the maximum period possible, i.e. 30 years.

The sponsor of the clinical trial must retain all other documentation pertinent to the trial as long as the product is authorised.

The sponsor or successor must retain the final report of products that are no longer authorised for five years.

## **Relevant standards and guidelines**

**35. BS ISO 15489-1** (Designing and Implementing Records Keeping Systems – DIRKS) Includes an eight step approach to effective records management for organisations to follow.

### **36. BSI PD 0016: 2001 Document scanning. Guide to scanning business documents**

This guide provides an insight into the processes of document scanning, explains the main features and benefits of different types of scanners and provides guidance to evaluate scanners to user requirements. Find out more [here](#)

### **37. BSI BIP 0008**

#### **BSI BIP [0008-1:2008](#)**

The current British Standard document relating to ‘Evidential Weight and Legal Admissibility of Information Stored Electronically’.

#### **BSI [BIP 0008-2:2008](#)**

The current British Standard document relating to ‘Evidential Weight and Legal Admissibility of Information Transferred Electronically.’

#### **BSI [BIP 0008-3:2008](#).**

The current British Standard document relating to ‘Evidential Weight and Legal Admissibility of Linking Electronic Identity to Documents’.

### **38. [BS 4783-8:1994](#)**

Storage, transportation and maintenance of media for use in data processing and information storage. Recommendations for 4 mm and 8 mm helical scan tape cartridges.

39. [BS 5454:2000](#) Recommendations for the Storage and Exhibition of Archival Documents.

40. [BS ISO/IEC 17799:2005 BS ISO/IEC 27001:2005 BS7799-2:2005](#)

This Standard provides a code of practice and a set of requirements for the management of information security.

The Standard is published in two parts. Part one has been adopted as ISO 17799:2000 and provides a code of practice for information security management. Part two provides a specification for information security management systems.

41. [PD ISO/TR 15489-2:2001](#)

This is the international records management standard and is about best practice in records management.

42. [BS ISO 19005-1:2005](#) – Document Management

This Standard provides for organisations to archive documents electronically for long-term preservation.

## **Professional Codes of Conduct and Guidance**

All the NHS professions have their own codes of conduct setting out the standards of ethical behaviour owed by members of each profession. These standards typically include:

- respecting patients' decisions about their care and treatment;
- obtaining consent for treatment or for disclosure of patient personal information;
- protecting patient personal information by maintaining confidentiality; and
- ensuring continuity of care through good record-keeping practice.

Information on professional codes of practice can be obtained from the following organisations

43. [The General Dental Council, Standards for Dental Professionals](#)

**(06/05)** The GDC guidance explains the standards the GDC expects of dental professionals:

**44. [The General Medical Council: Good Medical Practice](#) (2006)**

Good Medical Practice sets out the principles and values on which good practice is founded;

**45. [Health Professionals Council: Standards for Conduct, Performance and Ethics](#) (07/08)**

Explaining the standards of conduct, performance and ethics that registrants and prospective registrants must keep to.

**46. [The code: Standards of conduct, performance and ethics for nurses and midwives](#) NMC (01/08)**

Informs Nurse and Midwives of the standard of professional conduct required of them in the exercise of their professional accountability and practice.

**[Nursing and Midwifery Council: Standards for Medicine Management](#) (02/08)**

Includes records management guidance on transcribing medication from one "direction to supply or administer" to another form of "direction to supply or administer" and storage of medication and associated records.

**47. [Nursing and Midwifery Council, Record Keeping Guidance](#) (07/09)**

NMC guidance on records and record-keeping practices for nurses and midwives.

**48. Nursing and Midwifery Council : [Midwives' Rules and Standards - \(05/04\)](#)**

The Nursing and Midwifery Order 2001 requires the NMC to set rules and standards for midwifery, including record keeping.

**49. [The Chartered Society of Physiotherapy: Rules of Professional Conduct](#) (2005)**

**50. [The Chartered Society of Physiotherapy: General Principles of Record Keeping and Access to Health Records](#) (2000)**

**51. [Scottish Social Services Council: Codes of Practice for Social Service Workers and Employers](#) (2009)**

# ANNEX D – ‘THE MANAGEMENT, RETENTION AND DISPOSAL OF PERSONAL HEALTH RECORDS

## Introduction

### Scope of Schedule

This Annex sets out the minimum periods for which the various personal health records created within the NHS or by predecessor bodies should be retained (in line with Principle 5 of The Data Protection Act 1998), either due to their ongoing administrative value or as a result of statutory requirement. It also provides guidance on dealing with records which have ongoing research or historical value and should be selected for permanent preservation as archives and transferred to an appropriate archive.

The Annex provides information and advice about all personal health records commonly found within NHS organisations. The retention schedules apply to all the records concerned, irrespective of the format (e.g. paper, databases, e-mails, X-rays, photographs, CD-ROMs) in which they are created or held.

This Annex does not provide specific guidelines on determining which documents are retained as part of a personal health record. However, in Addendum 1, principles to be used in determining policy regarding the retention and storage of essential maternity records are set out. In addition, NHS organisations are reminded that good practice suggests that a policy determining which documents should remain in the record after discharge (or culling) should be in place. The development of such a policy should include addressing any clinical requirements for completeness of information, as well as the legal requirements of the Data Protection Act 1998, which states that only personal information which is relevant and not excessive should be retained.

Guidance on corporate (i.e. administrative, non-health) records commonly found within NHS organisations is given in [Annex E](#)



## **Responsibilities and Decision Making**

NHS Boards are public authorities in terms of the Freedom of Information (Scotland) Act 2002, and their records are covered by the provisions of that Act and its Code of Practice on Records Management (under section 61 of the Act).

For an NHS organisation to manage its records effectively, wider records management responsibilities need to be considered, placed with the appropriate individuals and/or committees, and resourced. For example, organisations may require local records managers and/or a corporate records manager; a health or medical records manager and/or committee; and an archivist.

In addition, NHS Boards are required to comply with the Information Governance standards set out in the Clinical Governance and Risk Assessment standards specified by NHS Quality Improvement Scotland. These include standards applicable to administrative and patient records.

## Retention Periods

Each organisation must produce its own retention schedule, specifying the locally agreed retention periods, in the light of its own internal requirements. Organisations must not apply to any records a shorter retention period than the minimum set out in this schedule, but there may be circumstances in which they need to apply a longer retention period. Organisations should ensure that they are able to justify, particularly in terms of the Data Protection Act when applicable, the retention of records for longer than the minimum period set out in this schedule. NHS Boards and GPs as producers of products and equipment, are affected by the provisions of the Consumer Protection Act 1987 covering the liability of producers for defective products. They may also be liable in certain circumstances as suppliers and users of products. An obligation for liability lasts for 10 years and within this period the Prescription and Limitation (Scotland) Act 1973, as amended by the Consumer Protection Act 1987, provides that the pursuer must commence any action within 3 years' from the date on which the pursuer was aware of the defect and aware that the damage was caused by the defect. This means that if a defective product was likely to have affected the health of a patient, then the patient's record would have to be retained for at least 13 years'. It will be for Boards and GPs to make their own judgement in such cases on whether any health records should be retained for this minimum period in order to defend any action brought under the Consumer Protection Act 1987. Organisations should ensure that they have mechanisms in place to identify records for which the appropriate minimum retention period has expired, in line with the 5th principle of the Data Protection Act 1998. It is acknowledged that organizations will have different mechanisms available to them in order to do this, and that these may vary depending on the medium on which the record is held. In relation to paper records in particular, it is acknowledged that organisations may 'batch' records together e.g. on an annual basis, in order to make disposal decisions. In such instances one approach to the calculation of minimum retention periods would be to base it on the beginning of the year after the last date on the record. For example, a file in which the first entry is in February 2001 and the last in September 2004, and for which the retention period is six years would be kept in its entirety at least until the beginning of 2011.

## **Disposal and Destruction of Personal Health Records**

### **Decision Making**

Staff in the operational area that ordinarily uses the records will usually be able to decide on their disposal and/ or destruction. Operational managers are responsible for making sure that all records are periodically and routinely reviewed to determine what can be disposed of or destroyed in the light of local and national guidance.

In respect of personal health records, the NHS Scotland Information Governance Standards require that NHS Boards establish a Patient Records Committee, which makes decisions on policy matters and which includes representation from clinical and non-clinical staff, and which is linked appropriately to other Information Governance Groups. Input from local healthcare professionals should be a key element of any records management strategy.

Once the appropriate minimum period has expired, the need to retain records further for local use should be reviewed periodically. Because of the sensitive and confidential nature of such records and the need to ensure that decisions on retention balance the interests of professional staff, including any research in which they are or may be engaged, and the resources available for storage, it is recommended that the views of the profession's local representatives should be obtained.

## Disposal and Destruction

At the end of the relevant minimum retention period, one or more of the following listed actions will apply:

**Review:** records may need to be kept for longer than the minimum retention period due to ongoing administrative and/ or clinical need. As part of the review, the organisation should have regard to the fifth principle of the Data Protection Act 1998, which requires that personal data is not kept longer than is necessary. If it is decided that the records should be retained for a period longer than the minimum the internal retention schedules will need to be amended accordingly and a further review date set. Otherwise, one of the following will apply:

**Transfer to or consult an NHS archivist or The National Archives of Scotland (see 'Archives' section below):** if the records have no ongoing administrative value but have, or may have, long-term historical or research value. Organisations that do not have their own archivist should consult an NHS Archivist or the National Archives of Scotland for advice.

**Destroy:** where the records are no longer required to be kept due to statutory requirement or administrative or clinical need, and they have no long-term historical or research value. In the case of personal health records, this should be done in consultation with clinicians in the organisation and archivists, with the necessary arrangements made to protect patient confidentiality where appropriate. It is important that records of destruction of health records contained in this retention schedule are retained permanently. No surviving health record dated 1948 or earlier should be destroyed. Organisations should also remember that records containing personal information are subject to the Data Protection Act 1998.

## Archives

All records management procedures with respect to NHS records, especially those that may be candidates for permanent preservation because of their wider medical or historical importance, should be informed by advice from the appropriate NHS Archivist or the National Archives of Scotland. (See the attached list of useful contacts in [Annex B](#).)

Every NHS Board should have access to the services of a professional archivist. A number of NHS Boards employ qualified archivists to look after their non-current health records and to make them available both to staff of the employing authority and members of the public in consultation with the Keeper of the Records of Scotland. In the case of Boards that do not have their own archivist, an NHS Archivist or the National Archives of Scotland will offer advice on request.

Where possible, the Schedule identifies those records likely to have permanent research and historical value. Beyond this, some NHS organisations will have particular and individual reasons, which relate to their own history, for retaining particular records as archives. Conversely, it should also be borne in mind that some records may have a long-term research value outside the NHS organisation that created them (e.g. both administrative and personal health records from a number of different hospitals have been used to study the 1918 influenza epidemic).

## Interpretation of the Schedule

The following types of record are covered by this retention schedule (regardless of the media on which they are held, including paper, electronic, images and sound, and including all records of NHS patients treated on behalf of the NHS in the private health sector):

- personal health records (electronic or paper-based, and concerning all specialties, including GP medical records);
- records of private patients seen on NHS premises;
- Accident and Emergency, birth and all other registers;
- theatre, minor operations and other related registers;
- xray and imaging reports, output and images;
- photographs, slides and other images;
- microform (i.e. microfiche/ microfilm);
- audio and video tapes, cassettes, CDROMS etc;
- emails;
- records held on computer; and
- scanned Documents.

The layout and some of the content of the schedule is based on that published by the Department of Health on 30 March 2006 in its publication: 'Records Management: NHS Code of Practice' (270422/2/Records Management: NHS Code of Practice Part 2). Find out more [here](#)

**The Schedule is organised into a table with 3 headings:**

RECORD TYPE: lists alphabetically records created as part of a particular function.

MINIMUM RETENTION PERIOD: specifies the shortest period of time for which the particular type of record is required to be kept. This period of time is usually set either because of statutory requirement or because the record may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision on its own retention schedule. In this regard, however, organisations must consider the fifth principle of the Data Protection Act 1998, i.e. that personal data should not be retained longer than is necessary.

NOTE: - provides further information, such as whether the record type is likely to have long-term research or historical value.

The following 'standard' retention periods apply to the following record types:

<b><i>Record Type</i></b>	<b><i>Minimum NHS Retention Period</i></b>
Adult	6 years after date of last entry or 3 years after death if earlier
All types of records relating to Children and young people (including children's and young person's Mental Health Records)	Retain until the patient's 25th birthday or 26th if young person was 17 at conclusion of treatment, or 3 years after death.  If the illness or death could have potential relevance to adult conditions or have genetic implications, the advice of clinicians should be sought as to whether to retain for a longer period.

<b>Record Type</b>	<b>Minimum NHS Retention Period</b>
Mentally disordered person (within the meaning of any Mental Health Act )	<p>20 years after date of last contact between the patient/ client/ service user and any health/ care professional employed by the mental health provider, or 3 years after the death of the patient/ client/ service user if sooner and the patient died while in the care of the organisation.</p> <p>N.B. NHS organisations may wish to keep mental health records for up to 30 years before review. Records must be kept as complete records for the first 20 years in accordance with this retention schedule but records may then be summarised and kept in summary format for the additional 10-year period.</p> <p>Social services records are retained for a longer period. Where there is a joint mental health and social care record, the higher of the two retention periods should be adopted.</p> <p>When the records come to the end of their retention period, they must be reviewed and not automatically destroyed. Such a review should take into account any genetic implications of the patient's illness. If it is decided to retain the records, they should be subject to regular review.</p>

Throughout this Schedule, where the 'standard' retention period specified above applies, the relevant record type has the entry 'Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)' in the 'Minimum Retention Period' column. Where it does not apply, the required minimum retention period is listed in the 'Minimum Retention Period' column.



## Health Records Retention Schedule

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
A&E records (where these are stored separately from the main patient record)	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
A&E registers (where they exist in paper format)	8 years after the year to which they relate.	Likely to have archival value- see footnote
Abortion – Certificates set out in Schedule 1 to the Abortion (Scotland) Regulations 1991	3 years beginning with the date of the termination	
Admission books (where they exist in paper format)	8 years after the last entry	Likely to have archival value- see footnote
Ambulance records – patient identifiable Component (including paramedic records made on behalf of the Ambulance Service)	7 years	
Asylum seekers and refugees (NHS personal health record – patient held record)	Special NHS record- patient held, no requirement on the NHS to retain.	
Audiology records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	

<b><i>TYPE OF HEALTH RECORD</i></b>	<b><i>MINIMUM RETENTION PERIOD</i></b>	<b><i>NOTE</i></b>
Birth registers (ie register of births kept by the hospital)	2 years	Likely to have archival value- see footnote
Body release forms	2 years	
Breast screening Xrays	8 years	
Cervical screening slides	10 years	
Chaplaincy records	2 years	Likely to have archival value- see footnote
Child and family guidance	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
Child Protection Register (records relating to)	Retain until the patient's 26th birthday	
Clinical audit records	5 years	
Clinical psychology	30 years	

<b><i>TYPE OF HEALTH RECORD</i></b>	<b><i>MINIMUM RETENTION PERIOD</i></b>	<b><i>NOTE</i></b>
Clinical trials of investigational medicinal products – health records of participants that are the source data for the trial	For trials to be included in regulatory submissions: At least 2 years after the last approval of a marketing application in the EU. These documents should be retained for a longer period, however, if required by the applicable regulatory requirement(s) or by agreement with the Sponsor. It is the responsibility of the Sponsor/someone on behalf of the Sponsor to inform the investigator/institution as to when these documents no longer need to be retained. <b>For trials which are not to be used in regulatory submissions:</b> At least 5 years after completion of the trial. These documents should be retained for a longer period if required by the applicable regulatory requirement(s), the Sponsor or the funder of the trial, In either case, if the period appropriate to the specialty is greater, this is the minimum retention period.	Likely to have research value see footnote
Counselling records	30 years	Likely to have research/ historical value see footnote
Death – Cause of, Certificate counterfoils	2 years	
Death registers – i.e. register of deaths kept by the hospital, where they exist in paper format	2 years	Likely to have archival value- see footnote

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Dental epidemiological surveys	30 years	
Dental, ophthalmic and auditory screening records	Adults: 11 years Children: 11 years, or up to 25th birthday, whichever is the longer	
Diaries – health visitors and district nurses	2 years after end of year to which diary relates. Patient relevant information should be transferred to the patient record.	It is not good practice to record patient identifiable information in diaries.
Dietetic and nutrition	Retain according to the standard minimum retention period appropriate to the patient/ specialty(see above)	
Discharge books (where they exist in paper format)	8 years after the last entry	Likely to have archival value-see footnote
District nursing records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
Donor records (blood and tissue)	30 years post transplantation	Likely to have research/ historical value see footnote
Family planning records	10 years after the closure of the case For children retain until their 25 <sup>th</sup> Birthday	

<b><i>TYPE OF HEALTH RECORD</i></b>	<b><i>MINIMUM RETENTION PERIOD</i></b>	<b><i>NOTE</i></b>
Forensic medicine records (including pathology, toxicology, haematology, dentistry, DNA testing, post mortems forming part of the Procurator Fiscal's report, and human tissue kept as part of the forensic record) See also Human tissue, Post mortem registers	For post mortem records which form part of the Procurator Fiscal's report, approval should be sought from the PF for a copy of the report to be incorporated in the patient's notes, which should then be kept in line with the specialty, and then reviewed.  In cases where criminal proceedings are anticipated documentation is not normally entered in to the patient records.  All other records retain for 30 years.	Likely to have research/ historical value see footnote
Genetic records	30 years from date of last attendance.	Likely to have research/ historical value see footnote
Genito Urinary Medicine (GUM)	Store according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	

<b><i>TYPE OF HEALTH RECORD</i></b>	<b><i>MINIMUM RETENTION PERIOD</i></b>	<b><i>NOTE</i></b>
<p>GP records, including medical records relating to HM Armed Forces</p>	<p>Retain for the lifetime of the patient and for 3 years after their death.</p> <p>Records relating to those serving in HM Armed Forces - The Ministry of Defence (MoD) retains a copy of the records relating to service medical history. The patient may request a copy of these under the Data Protection Act (DPA), and may, if they choose, give them to their GP. GPs should also receive summary records when ex-Service personnel register with them. What GPs do with them is a matter for their professional judgement, taking into account clinical need and Data Protection Act requirements- they should not, for example, retain information that is not relevant to their clinical care of the patient.</p> <p>GP records of serving military personnel in existence prior to them enlisting must not be destroyed. Following the death of the patient the records should be retained for 3 years.</p> <p>*Electronic Patient Records (EPRs)- GP only- must not be destroyed, or deleted, for the foreseeable future</p>	<p>*The rationale for this is explained in 'SCIMP Good Practice Guidelines for General Practice Electronic Patient Records – section 6.1'</p>

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Health visitor records	10 years Records relating to children should be retained until their 25th birthday	
Homicide/ 'serious untoward incident' records	30 years	Likely to have research/ historical value see footnote
Hospital acquired infection records	6 years	
Human fertilisation records, including embryology records	<p>Treatment Centres</p> <ol style="list-style-type: none"> <li>1. If a live child is not born, records should be kept for at least 8 years after conclusion of treatment</li> <li>2. If a live child is born, records shall be kept for at least 25 years after the child's birth</li> <li>3. If there is no evidence whether a child was born or not, records must be kept for at least 50 years after the information was first recorded</li> </ol> <p><b>Storage Centres</b></p> <p>Where gametes etc have been used in research, records must be kept for at least 50 years after the information was first recorded.</p> <p><b>Research Centres</b></p> <p>Records are to be kept for 3 years from the date of final report of results/ conclusions to Human Fertilisation and Embryology Authority (HFEA)</p>	Likely to have research value see footnote

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Human tissue (within the meaning of the Human Tissue (Scotland) Act 2006) (see Forensic medicine above)	For post mortem records which form part of the Procurator Fiscal's report, approval should be sought from the Procurator Fiscal for a copy of the report to be incorporated in the patient's notes, which should then be kept in line with the specialty, and then reviewed.	Likely to have research value see footnote
Intensive Care Unit charts	Retain according to the standard minimum retention period appropriate to the patient/specialty (see above)	
Joint replacement records	For joint replacement surgery the revision of a primary replacement may be required after 10 years to identify which prosthesis was used. Only need to retain minimum of notes with specific information about the prosthesis.	Likely to have research value see footnote
Learning difficulties – (records of patients with)	Retain for 3 years after the death of the individual.	
Macmillan (cancer care) patient records –community and acute	Retain according to the standard minimum retention period appropriate to the patient/specialty (see Above)	



<b><i>TYPE OF HEALTH RECORD</i></b>	<b><i>MINIMUM RETENTION PERIOD</i></b>	<b><i>NOTE</i></b>
Maternity (all obstetric and midwifery records, including those of episodes of maternity care that end in stillbirth or where the child later dies)	25 years after the birth of the last child	
Medical illustrations (see Photographs below)	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Mentally disordered persons (within the meaning of any Mental Health Act )	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Microfilm/ microfiche records relating to patient care	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	Likely to have archival value- see footnote
Midwifery records	25 years after the birth of the last child	
Mortuary registers (where they exist in paper format)	10 years	Likely to have research/ historical value see footnote
Music therapy records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Neonatal screening records	25 years	
Notifiable diseases book	6 years	
Occupational Health Records (staff)	6 years after termination of employment	
Health Records for classified persons under medical surveillance	50 years from the date of the last entry or age 75, whichever is the longer	Likely to have research/historical value see footnote
Personal exposure of an identifiable employee monitoring record	40 years from exposure date	Likely to have research/historical value see footnote
Personnel health records under occupational surveillance	40 years from last entry on the record	Likely to have research/historical value see footnote
Radiation dose records for classified persons	50 years from the date of the last entry or age 75, whichever is the longer	Likely to have research/historical value see footnote

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Occupational therapy records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Oncology (including radiotherapy)	30 years N.B. Records should be retained on a computer database if possible. Also consider the need for permanent preservation for research purposes.	Likely to have research value see footnote
Operating theatre registers	8 years after the year to which they relate	Likely to have historical value- see footnote
Orthoptic records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Out of hours records (GP cover), including video, DVD and tape voice recordings	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Outpatient lists (where they exist in paper format)	2 years after the year to which they relate	
Parent held records	There should be a copy kept at the NHS organisation responsible for delivering that care and compiling the record of the care.  The records should then be retained until the patient's 25th birthday, or 26th birthday if the young person was 17 at the conclusion of treatment, or 3 years after death	

## Pathology records: Documents, electronic and paper

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Accreditation documents; records of Inspections	10 years or until superseded	
Batch records results	10 years	
Bound copies of reports / records, if made	30 years	
Correspondence on patients	This should be lodged in the patient's record, if feasible. However this is often beyond the control of the laboratory, particularly for case referred distantly, and ensuring entry into the patients notes is not primarily the responsibility of laboratory staff. Otherwise, keep for at least 30 years; this may be most conveniently done in association with stored paper or scanned copy of the relevant specimen request and/ or report kept by the relevant laboratory.	
Day books and other records of specimens received by a laboratory	2 years from specimen receipt	
Equipment/ instruments maintenance logs, records of service inspections	Lifetime of instrument; minimum of 10 years	
Procurement, use, modification and supply records relevant to production of products (diagnostics) or equipment	Comprehensive records relevant to procurement, use, modification and supply: 10 years.	

***Pathology records: Documents, Electronic and Paper Records***

<b><i>TYPE OF HEALTH RECORD</i></b>	<b><i>MINIMUM RETENTION PERIOD</i></b>	<b><i>NOTE</i></b>
External quality control Records	Subscribing laboratories or individuals, 5 years to ensure continuity of data available for laboratory accreditation purposes. Records will be kept for longer periods by organisations providing external quality assessment schemes.	
Internal quality control Records	10 years	
Lab file cards or other working records of test results for named patients	1 year from specimen receipt if all results transcribed into a separately issued and stored formal report. Otherwise, they should be kept as for worksheets over. The diversity of these types of working records is very wide; within specialties and departments, consideration should be given to the potential audit or medico-legal value of storing such working records for 30 years, as for other primary records.	
Mortuary Registers	30 years	
Near-patient test data	Result in patient record, log retained for lifetime of instrument	
Pathological archive/museum catalogues	For as long as the specimens are held or until the catalogue is updated, subject to consent where required, (with maintained and accessible documentation of consent)	

***Pathology records: Documents, Electronic and Paper Records***

<b><i>TYPE OF HEALTH RECORD</i></b>	<b><i>MINIMUM RETENTION PERIOD</i></b>	<b><i>NOTE</i></b>
Photographic records	Where images represent a primary source of information for the diagnostic process, whether conventional photographs or digital images, they should be kept for at least 30 years.	
Records of telephoned Reports	Note of the fact and date/ time that a telephone or fax report has been issued should be added to the laboratory electronic records of the relevant report, or to hard copies and kept for a minimum of 5 years. Where management advice is discussed in telephone calls, a summarised transcript should be retained long term, as for the retention of other correspondence. Clinical information or management advice provide by fax, in addition of pure transmission of report, should also be kept as correspondence in the patient note and/ or stored with a laboratory copy of the specimen request/ report for 30 years.	
Records relating to cell/ tissue transplantation	Records not otherwise kept or issued to patient records that relate to investigations or storage of specimens relevant to cell/ tissue transplantation, including donated organs from deceased individuals should be kept for at least 30 years or the lifetime of the recipient, whichever is the longer.	

***Pathology records: Documents, Electronic and Paper Records***

<b><i>TYPE OF HEALTH RECORD</i></b>	<b><i>MINIMUM RETENTION PERIOD</i></b>	<b><i>NOTE</i></b>
Records relating to investigation or storage of specimens relevant to organ transplantation, semen or ova	30 years if not held with health record	
Reports and copies (physical or electronic)	6 months or as needed for operational procedures. Where copies represent a means of communication or aide memoire, for example at a multi- disciplinary meeting or case conference, they may be disposed of when that function is complete. Copies of reports sent by fax, with accompanying details of the date and times of transmission, and the intended recipient, should be retained in conjunction with the matching specimen reports and stored long-term by the laboratory. Any such copies generated to substitute for an original report (e.g. if an original is misplaced) should be retained as for the original.	
Reports, copies Post mortem reports	The report should be lodged in patient's record; in the case of Procurator Fiscal reports this is dependant on the PF's approval. Electronic or hard copy should be kept at least 30 years with maintained accessibility. In addition to accessible indexing of paper copies, there must be continuation of access to e-copies when laboratory, computer systems are upgraded or replaced. This guidance applies equally to rapid, short reports that maybe prepared for the PF, summarising cause of death and to the final reports of post-mortem examinations.	

***Pathology records: Documents, Electronic and Paper Records***

<b><i>TYPE OF HEALTH RECORD</i></b>	<b><i>MINIMUM RETENTION PERIOD</i></b>	<b><i>NOTE</i></b>
Request forms that are not a unique record	Request forms should be kept until the authorised report, or reports on investigation arising from it, have been received by the requestor. As this period of time may vary with local circumstances, no minimum retention time is recommended, request forms need not to be kept for more than one month after the final checked report has been despatched. For many uncomplicated requests, retention of 1 week will suffice.	
Request forms that contain clinical information not readily available in the health record	30 years Where the request form is used to record working notes or as a worksheet, it should be retained as part of the laboratory record.	
Standard operating procedures (both current and outdated protocols)	30 years	
Surgical (histological) reports	Copy lodged in patients notes. Electronic or hard copy to be kept for at least 30 years by the laboratory with maintained accessibility of e- copies when laboratory, computer systems are upgraded or replaced.	



## Pathology Records: Specimens and Preparations.

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Body fluids/ aspirates/ swabs	Keep for 48 hours after the final report has been issued by the laboratory, unless sample deterioration precludes storage.	
Blocks for electron microscopy	30 years	
Electrophoretic strips and immunofixation plates	Keep for 5 years, unless digital images are taken, if digital images of adequate quality for diagnosis are taken, then the original preparations may be discarded after 2 years. The images should then be stored under "photographic records" bearing in mind the need to maintain the ability to read archived digital images when equipment is updated.	
Foetal serum	Because of its rarity and value for future research, wherever possible foetal serum should be kept for at least 30 years.	
Frozen tissue for immediate histological assessment (frozen section)	Stained microscope slides should be kept for a minimum of 10 years.	
Frozen tissues or cells for histochemical or molecular genetic analysis	10 years and preferably longer if storage facilities permit.	
Grids for electron microscopy	Requirements in different specialties differ. Grids prepared for human tissue diagnosis (e.g. renal, muscle, nerve, or tumour) should be kept for 10 years; preferably longer if practicable. Grids prepared for virus identification may be discarded 48 hours after the final report has been issued, provided that all derived images are retained and remain accessible for at least 30 years.	

<b>Pathology Records Specimens and Preparations</b>		
<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Human DNA	4 weeks after final report for diagnostic specimens. 30 years for family studies for genetic disorders (consent required)	
Microbiological cultures	24-28 days after final report of a positive culture issued. 7 days for certain specified cultures- see RCPATH document	
Museum specimens (teaching collections)	Permanently. Consent of the relative is required if it is tissue	
Newborn blood spot screening cards	A minimum of 5 years storage is indicated for quality assurance purposes, with longer term storage recommended in accordance with the Code of Practice of the U.K Newborn Screening Programme Centre (2005). See <a href="#">here</a> for more information.	
Paraffin blocks	Storage for at least 30 years is recommended, if facilities permit. If not, review the need for archiving at 10 years (and at similar intervals thereafter) and select representative blocks, showing the relevant pathology for permanent retention. Blocks representing rare pathologies and those (including representative normal tissue) from patients of diseases known or thought likely to have an inherited genetic predisposition should be particularly considered for permanent retention. Wherever possible, storage of all histology block should be for the full minimum of 30 years.	
Plasma and serum	Keep for 48 hours after the final report has been issued by the laboratory.	

<b>Pathology Records Specimens and Preparations</b>		
<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Records relating to donor or recipient sera	Serum samples obtained from recipient (s) for the purposes of matching in cell/tissue transplantation, and their accompanying records, must be kept for the lifetime of the recipient.	
Serum from first pregnancy booking visit	Should be kept by microbiology/ virology and other relevant laboratories to provide a baseline for further serological or other tests for infections or other disease during pregnancy and the first 12 months after delivery. Because of rarity and value to future research, wherever possible, foetal serum (from cordocentesis) should be kept for at least 30 years.	
Stained slides	Appropriate retention times depend on there nature and purpose. Relevant guidance on minimum retention periods can be found <a href="#">here</a> . Note that where sections are likely to contain intact human cells, or are intended to be representative of whole cells, they constitute “relevant material” under the Human Tissue act 2004; further information can be found <a href="#">here</a> .	
Wet tissue (representative aliquot or whole tissue or organ)	For surgical specimens from living patients, keep for 4 weeks after issue of final report. For cases in which a supplementary report is anticipated after additional tests, (such as various molecular investigations or referral for expert opinion), which may occasionally exceed this period, arrangements should exist to ensure that individual specimens are retained until the additional report has been finalised.	
Whole blood samples, for full blood count	24 hours	

## Pathology Records: Transfusion Laboratories

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Annual reports (where required by EU directive)	15 years	
Autopsy reports, specimens, archive material and other where the deceased has been the subject of Procurator Fiscals autopsy	Procurators Fiscal have absolute dominion over autopsy reports. They are confidential to them and may not be released without their consent to any third party. It is good practise to lodge copies of the autopsy report in the deceased patients health record but the consent of the procurator fiscal should be obtained.	
Blood bank register, blood component audit trail and fates	30 years to allow full traceability of all blood products used. The data may be held in electronic form if robust archiving arrangements are in place. For hospital laboratories the records should include: Blood component supplier identification. Issued blood component identification Transfused recipient identification For blood units not transfused; confirmation of subsequent disposition (discard/ other use) Lot number (s) of derived component (s) if relevant Date of transfusion or disposition (day, month and year)	
Blood for grouping, antibody screening and saving and/or cross-matching	1 week at 4° C	

**Pathology Records: Transfusion Laboratories**

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Forensic material – criminal cases	Permanently- not part of the health record. In cases where criminal proceeding can be anticipated, all recording made at the autopsy, be the hand written notes (by everyone, i.e. pathologist, technician, trainee, etc), tape recordings, drawings or photographs, are all documentary records and as such their existence must be declared (disclosed). They must be available to all involved throughout the lifetime of the case, including appeals and other re-investigations.	
Refrigeration and freezer charts	15 years	
Request forms for grouping, antibody screening and cross-matching	1 month	
Results of grouping, antibody screening and other blood transfusion-related tests	30 years to allow full traceability of all blood products used, in compliance with the Blood Safety and Quality Regulations 2005.	
Separated serum/plasma, stored for transfusion purposes	No minimum storage time is recommended for recipient patient samples. Storage of donated serum/ plasma should optimally be at -30 degrees Centigrade or colder. These materials may be stored for up to 6 months, but guidelines for the timeline of sample collection prior to blood transfusion must be followed. Archived blood donor samples should be stored by blood services for at least 3 years, and preferable longer if it is practicalable, in order to facilitate 'look back' exercises.	

<b>Pathology Records: Transfusion Laboratories</b>		
<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Storage of material following analyses of nucleic acids	Developing technologies mean that there are now a variety of hard copy and / or electronic outputs associated with the analysis and interpretation of diagnostic tests using nucleic acid. It is recommended that all such outputs should be stored for at least 30 years unless the information is transcribed into permanently accessible report formats authorised by senior clinical laboratory staff or pathologists. The later reports should be kept for at least 30 years, as for other pathology reports may be regarded as reporting documents. For such working documents storage for at least the instrument , with a minimum of 10 years is recommended.	
Worksheets	30 years to allow full traceability of all blood products used	
<b>End of Pathology Records</b>		

### **Patient Held Records**

Patient held records	At the end of an episode of care the NHS organisation responsible for delivering that care and compiling the record of the care must make appropriate arrangements to retrieve patient-held records. The records should then be retained for the period appropriate to the patient/ specialty (see Above).	
----------------------	--	--

## Pharmacy Records: Prescriptions

<b><i>TYPE OF HEALTH RECORD</i></b>	<b><i>MINIMUM RETENTION PERIOD</i></b>	<b><i>NOTE</i></b>
Chemotherapy	2 years after last treatment	
Clinical drug trials (non-sponsored)	2 years after completion of trial	
GP10, TTO's, outpatient, private	2 years	N.B. Inpatient prescriptions held as part of health record.
Immunoglobulin's/ blood products	30 years	To allow full traceability of all blood products used
Parenteral nutrition	2 years	Original valid prescription to be held with the health record.
Unlicensed medicines dispensing record	5 years	

## Pharmacy Records: Clinical trials

<b><i>TYPE OF HEALTH RECORD</i></b>	<b><i>MINIMUM RETENTION PERIOD</i></b>	<b><i>NOTE</i></b>
Destruction records	2 years after end of trail	
Dispensing records	2 years	
Production batch records	5 years after end of trial	
Protocols	2 years	

## Pharmacy Records: Worksheets

<b><i>TYPE OF HEALTH RECORD</i></b>	<b><i>MINIMUM RETENTION PERIOD</i></b>	<b><i>NOTE</i></b>
Chemotherapy, aseptics worksheets,	5 years	
Extemporaneous dispensing records	5 years	
Parenteral nutrition, production batch records	5 years	
Production batch records	5 years	
Raw material request and control forms	5 years	
Resuscitation box worksheet	1 year after the expiry of the longest data item Applies only to re-packaged items.	
Paediatric worksheets	As per Children and Young People (see Above)	



## Pharmacy Records: Quality Assurance

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Analysis certificates	5 years or 1 year after expiry date of batch (whichever is longer)	
Environmental monitoring results	1 year after expiry date of products	As electronic record in perpetuity
Equipment validation	Lifetime of the equipment	
Operators validation	Duration of employment	
QC Documentation,	5 years or 1 year after expiry date of batch (whichever is longer)	
Refrigerator temperature	1 year	Refrigerator records to be retained for the life of any product stored therein particularly vaccines
Standard operating procedures	15 years after superseded by revised version	As electronic record in perpetuity

## Pharmacy Records: Orders

Adhoc forms (dispensing requests forms to store)	3 months	
Invoices	6 years	
Order and delivery notes, requisition sheets, old order books	Current financial year plus one	
Picking tickets/ delivery notes	3 months	
Ward Pharmacy requests	1 year	

## Pharmacy Records: Controlled Drugs, Others

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Aspetic controlled drugs worksheets (paediatric)	26 years	
Controlled drugs, Clinical trails	5 Years	
Controlled drug destruction records (pharmacy based)/ destruction of patients' own CD's	7 years	
Controlled drug prescriptions (TTOs/OP)	2 years	
Controlled drug order books, ward orders and requisitions	2 years from date of last entry	
Controlled drug registers (pharmacy and ward based)	2 years from date of last entry, but if contain record of destruction of CD, keep for 7 years	
Copy of signature for CD ward order or requisition	Duration of employment	Copy of signature of each authorised signatory should be available in the pharmacy department
Extemporaneous controlled drugs preparation worksheets	13 years	
External controlled drug orders and delivery notes	2 years	

<b>Pharmacy records: others</b>		
Destruction of patients' own drugs	6 months	
Dispensing errors	1 year plus current	
Doctors/ nurses signatures	Duration of contract plus one year	
Medicines information enquiry	8 years (25 years for child obstetrics and gynaecology enquiries)	
Minor clinical interventions	2 years	
Recall documentation	5 years	
Stock check list	1 year plus current	
Superseded group directions	10 years	
Superseded intravenous drug administration monographs	5 years	
<b>(end of Pharmacy)</b>		

### Other Health Records

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Photographs (where the photograph refers to a particular patient it should be treated as part of the health record)	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Physiotherapy records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Podiatry records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Post mortem records (see Pathology records)		
Post mortem registers (where they exist in paper format)	30 years	Likely to have archival value- see footnote
Private patient records admitted under section 57 of the National Health Service (Scotland) Act 1978 or section 5 of the National Health Service (Scotland) Act 1947 (now repealed)	It would be appropriate for authorities to retain these according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
Psychology Records	30 years	Likely to have research/ historical value see footnote
Records/documents related to any litigation	As advised by the organisation's legal advisor. All records to be reviewed.	Likely to have research/ historical value see footnote
Records of destruction of individual health records (case notes) and other health related records contained in this retention schedule (in manual or computer format)	Permanently	Likely to have research/ historical value see footnote

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
<p>Research records</p> <p>1. Other than clinical trials of investigational medicinal products, health records of participants that are the source data for the research</p>	<p>30 years</p>	<p>See Footnote</p> <p>Review patient identifiable records every 5 years to see if they need to be retained or if their identifiably could be reduced.</p>
<p>2. Research records and research databases (not patient specific)</p>	<p>Clinical trials of investigational medicinal products</p> <p>At least 2 years after the last approval of a marketing application in the EU. These documents should be retained for a longer period, however, if required by the applicable regulatory requirement(s) or by agreement with the sponsor. It is the responsibility of the sponsor/ someone on behalf of the sponsor to inform the investigator/ institution as to when these documents no longer need retained.</p> <p>Research records other than for clinical trials of investigational medicinal products</p> <p>As above.</p>	<p>Likely to have research value</p> <p>see footnote</p>

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Scanned records relating to patient care	Retain in main records and retain for the period of time according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
School health records (see Children and young people)	Retain in Child Health Records	
Speech and language therapy records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
Telemedicine records (see also Video records)	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
Transplantation records	Records not otherwise kept or issued to patient, records that relate to investigations or storage of specimens relevant to organ transplantation should be kept for 3 years	Likely to have research value see footnote
Ultrasound records (e.g. vascular, obstetric)	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Video records/ voice recordings relating to patient care/videoconferencing records (see also Telemedicine records and Out of hours records)	<p>6 years subject to the following exceptions:</p> <p><b>Children and Young People-</b> Records must be kept until the patient's 25th birthday, if the patient was 17 at the conclusion of treatment until their 26th birthday, or until 3 years after the patient's death if sooner.</p> <p><b>Maternity-</b> 25 years</p> <p><b>Mentally disordered persons-</b> Records should be kept for 20 years after the date of last contact between patient/ client/ service user and any healthcare professional or 3 years after the patient's death if sooner.</p> <p><b>Cancer patients-</b> Records should be kept until 6 years after the conclusion of treatment, especially if surgery was involved. The Royal College of Radiologists has recommended that such records be kept permanently where chemotherapy and/ or radiotherapy was given.</p>	The teaching and historical value of such recordings should be considered, especially where innovative procedures or unusual conditions are involved. Video/ video-conferencing records should be either permanently archived or permanently destroyed by shredding or incineration (having due regard to the need to maintain patient confidentiality)
Ward registers, including daily bed returns (where they exist in paper format)	2 years after the year to which they relate	Likely to have archival value- see footnote

<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Xray films (excluding PACS images)	The minimum retention period for these can continue to be determined locally by the NHS organisation responsible. In setting the minimum retention period, appropriate recognition should be given to current professional guidance, clinical need, special interest groups, cost of storage and the availability of storage space.	
Xray – PACS images	<p>National: PACS images captured as part of the national PACS programme are stored in a central national archive in accordance with the National PACS for Scotland Image Retention/ Storage Policy, which is subject to annual review by the PACS Clinical Advisory Group.</p> <p>Local: Locally set minimum retention periods can continue to apply to PACS images that are not captured as part of the national PACS programme.</p>	As eHealth strategic developments progress, this guidance, along with that for other record types affected, will be reviewed.
Xray registers (where they exist in paper format)	30 years	Likely to have archival value- see footnote



<b>TYPE OF HEALTH RECORD</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>NOTE</b>
Xray reports (including reports for all imaging modalities)	To be considered as part of the patient record. Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	

**Foot Note** - record is likely to have permanent research and historical value, consult NHS archivist or National Archives of Scotland.

### **Principles to be used in Determining Policy Regarding the Retention and Storage of Essential Maternity Records**

Reproduced below is the joint position on the retention of maternity records as agreed by the British Paediatric Association, the Royal College of Midwives, the Royal College of Obstetricians and Gynaecologists and the then United Kingdom Central Council for Nursery, Midwifery and Health Visiting. This is specified in the Department of Health publication: 'Records Management: NHS Code of Practice' (270422/2/Records Management: NHS Code of Practice Part 2).

#### **Joint Position on the Retention of Maternity Records**

All essential maternity records should be retained. 'Essential' maternity records mean those records relating to the care of a mother and baby during pregnancy, labour and the puerperium.

Records that should be retained are those that will, or may, be necessary for further professional use. 'Professional use' means necessary to the care to be given to the woman during her reproductive life, and/or her baby, or necessary for any investigation that may ensue under the Congenital Disabilities (Civil Liabilities) Act 1976, or any other litigation related to the care of the woman and/or her baby.

Local level decision making with administrators on behalf of the health authority must include proper professional representation when agreeing policy about essential maternity records. 'Proper professional' in this context

should mean a senior medical practitioner(s) concerned in the direct clinical provision of maternity and neonatal services and a senior practising midwife. Local policy should clearly specify particular records to be retained AND include detail regarding transfer of records, and needs for the final collation of the records for storage. For example, the necessity for inclusion of community midwifery records.

The policy should also determine details of the mechanisms for the return, collation and storage of those records, which are held by mothers themselves, during pregnancy and the puerperium.

### **List of Maternity Records to be retained**

Maternity Records retained should include the following:

- documents recording booking data and pre-pregnancy records where appropriate;
- documentation recording subsequent antenatal visits and examinations;
- antenatal inpatient records;
- clinical test results including ultrasonic scans, alphafeto protein and chorionic villus sampling;
- blood test reports;
- all intrapartum records to include initial assessment, partograph and associated records including cardiotocographs;
- drug prescription and administration records;
- postnatal records including documents relating to the care of mother and baby, in both the hospital and community settings.

# **ANNEX E- ADMINISTRATIVE RECORDS**

## **RETENTION SCHEDULE**

This schedule sets out minimum periods for which the various administrative records created within the NHS or predecessor bodies should be retained (in line with the Principle 5 of The Data Protection Act 1998), either due to their ongoing administrative value or as a result of statutory requirement. Records are listed alphabetically within each record category, e.g. financial, human resources. The retention schedules apply to all the records concerned, irrespective of the format (e.g. paper, databases, emails, photographs, CD ROMs) in which they are created or held.

The review, to be undertaken by local organizations, will determine whether records are to be selected for permanent preservation, destroyed or retained for research or litigation purposes.

Whenever the schedule is used, the guidelines listed below should be followed:

- i. The minimum retention periods in this schedule must be adopted. However, local business requirements or risk analysis may require some categories of record to be kept for longer.
- ii. Recommended minimum retention periods should be calculated from the end of the calendar or accounting year following the last entry on the document.
- iii. The provisions of the Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002 must be observed. Decisions should also be considered in the light of the need to preserve records that may be in the substantial public interest or in relation to research purposes (Section 33(3) contains some exemptions from the 5th principle of the Data Protection Act 1998.) This applies to records whose use cannot be anticipated fully at the present time, but which may be of value to future generations.

iv. Some classes of document must be permanently preserved and the advice of the local NHS archivist, NAS (National Archives of Scotland) or the Scottish Government eHealth Directorate regarding an appropriate place of deposit should be obtained.

v. The selection of records for permanent archival preservation is partly informed by precedent (the establishment of a continuity of selection) and partly by the historical context of the subject (the informed identification of a selection). It is also possible to retain a sample of certain record series. General rules should be drawn up locally, using the profile of material that has already been selected, and the history of the institution or organisation (including pioneering treatments and examples of excellence) within the context of its service to the local and wider communities.

vi. Files and documents which, having been retained for the minimum retention period, are selected for destruction, should be destroyed appropriately, with particular regard being to whether the information contained in them is of a confidential or sensitive nature.

## Administrative Records - General

<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Conferences: lectures given by staff at other conferences	permanent	Significant conference papers should be selected for permanent retention
Conferences: organised by Boards – conference proceedings	permanent	
Conferences: organised by Boards - routine paperwork	destroy after conference	
Conferences: other conferences attended by staff	2 years	
Copies of out-letters (“flimsies”)	1 year	
Databases- records handling system	permanent	Retain to demonstrate implementation of established practice and provide audit trail, see also Indexes
Diaries - office	1 year after completion	
Indexes- file and document lists marked for permanent preservation	permanent	
Indexes- file and document lists not marked for permanent preservation	Destroy when no longer useful	Retention may be required if they are part of audit trails
Quality Assurance Records	12 years	

**Administrative Records: General**

<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Receipts for registered and recorded delivery mail	2 years	
Records of custody and transfer of keys	2 years	
Research and development findings by Board staff (scientific, technological and medical)	Consider findings and reports for permanent preservation	Supporting records should be retained in line with the appropriate clinical, pharmaceutical, laboratory or other research standards, as set out by funding and professional bodies.
Software licenses	Operational lifetime of product	

## Administrative Records - Financial

<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES SEE FOOT NOTE</b>
Accounts – final annual master copies	permanent	
Accounts - cost	3 years	
Accounts - working papers	3 years	
Accounts - minor records: (including pass books, paying-in slips, cheque counterfoils, cancelled/discharged cheques, petty cash expenditure, travelling and subsistence accounts, minor vouchers, duplicate receipt books, income records, laundry lists)	3 years after completion of audit	See 'Receipts for cheques bearing printed receipts' below
Accounts - statutory final	permanent	
Advice Notes	3 years after formal clearance by statutory auditor	A longer period may be required for investigative purposes
Audit records - original documents	3 years after formal clearance by statutory auditor	A longer period may be required for investigative purposes
Audit reports (including Management letters, VFM reports and system/final accounts memorandum)	3 years after formal clearance by statutory auditor	A longer period may be required for investigative purposes

**Administrative Records: Financial**

<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Bank statements	3 years after completion of audit	
Benefactions – endowments, legacies gifts etc.	permanent	
Bills and receipts	6 years	
Budget monitoring reports	3 years	
Budgets	2 years after completion of audit	
Capital paid invoices	3 years	See 'Invoices' below
Cash books and sheets	6 years	
Cost accounts		See 'Accounts' above
Creditor payments	3 years	
Debtors' records - cleared	6 years	
Debtors' records - uncleared	6 years	
Demand Notes	6 years	
Expenses claims		See 'Accounts – minor' above
Financial plans, estimates recovery plans	6 years	
Funding data	6 years	
General ledgers	6 years	
Income and expenditure sheets and journals	6 years	
Indemnity Forms	6 years after the indemnity has lapsed	



**Administrative Records: Financial**

<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Inquiries involving fraud/other irregularities	10 years	Where action is in prospect or has been commenced, consult with legal representatives and NHS Counter Fraud Services and keep in accordance with advice provided
Invoices payable (creditors)	6 years	
Invoices receivable (debtors)	6 years	
Ledgers	6 years	See also 'General ledgers' above
Mortgage documents - acquisition, transfer and disposal	permanent	
Non-exchequer funds records		See 'Income and expenditure journals' above
PAYE records	6 years	
Receipts	6 years	Includes cheques bearing printed receipts
SFR returns	6 years	
Superannuation - accounts and registers	10 years	
Superannuation - forms	10 years	
Tax forms	6 years	
VAT records	6 years	In some instances a shorter period may be allowed, but agreement must be obtained from HM Revenue and Customs

<i>Administrative Records: Financial</i>		
<i>TYPE/ SUBTYPE OF RECORDS</i>	<i>MINIMUM RETENTION PERIODS</i>	<i>NOTES</i>
Wages/salary records	10 years	For superannuation purposes authorities, may wish to retain such records until the subject reaches pensionable age

The Scottish Government policy on retention of financial records is set out in the Scottish Public Finance Manual, which can be accessed at:

<http://www.scotland.gov.uk/library5/finance/spfm/spf-00.asp>

## Administrative Records - Property, Environment and Health & Safety

<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Agreements	See 'Contracts' below	
Buildings - papers relating to occupation	Permanent or until property demolished or disposed	Does not include Health & Safety information
Capital charges data	3 years after completion of previous 5 year valuation term	
Contaminated Land	permanent	
Contracts - non sealed (property) on termination	6 years	
Environmental Information	permanent	
Equipment		See 'Products – liability' under 'Procurement Records'
Estimates: including supporting calculations and statistics	3 years	
Green code	permanent	
Health and safety: Asbestos Register	permanent	
Health and safety: Audit forms, COSHH (Control of Substances Hazardous to Health Regulations) documentation, safety risk data sheets, risk assessments and control measures etc.	10 years	
Health and Safety: Accident and Incident Forms	10 years	See 'Litigation dossiers' under 'NHS Board Records'

<b>Property, Environment and Health and Safety Records</b>		
<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Health and Safety: Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) including Accident Register	10 years	
Inspection Reports - e.g. boilers, lifts etc.	2 years after operational lifetime of installation / plant	Should be retained indefinitely if there is any measurable risk of a liability
Inventories (non-current) of items having an operational lifetime of less than 5 years	2 years	
Land purchase and sale - deeds, leases, maps, surveys, registers etc	permanent	
Land purchase and sale - negotiations not completed	6 years	
Laundry lists		See 'Accounts – minor' under 'Financial Records'
Manuals - operating		See 'Inspection reports' above
Manuals- policy and procedure	permanent	
Maintenance contracts		See 'Property- Cleaning and Maintenance' below

<b>Property, Environment and Health and Safety Records</b>		
<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Maintenance request book	2 years after financial year referred to	
Maps	consider for permanent preservation	
Project files (£250,000 and over)	permanent	Including abandoned or deferred projects
Project files (under £250,000)	6 years after completion / abandonment of project	
Project team files (£250,000 and over)	3 years	
Project team files (under £250,000)	3 years	
Property- acquisition dossiers	permanent	
Property - cleaning and maintenance (contracts less than £100,000)	6 years	
Property - disposal dossiers	permanent	
Property/ Estates- Land, Building and Engineering Construction Procurement: Key records (including: final accounts, surveys, site plans, bills of quantities, PFI/PPP records) Town and country planning matters and all formal contract documents (including: executed agreements, conditions of contract, specifications, "as built" record drawings and documents on the appointment and conditions of engagement of private buildings and engineering consultants)	permanent	Inclusive of major projects abandoned or deferred

**Property, Environment and Health and Safety Records**

<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Property - leases	permanent	
Property management system	permanent	
Property - minor contracts	6 years	
Property performance	permanent	
Property - purchases	permanent	
Property strategy	permanent	
Property - title deeds	permanent	
Property- terriers (NHS premises site information)	permanent	
Safety Action Bulletins	Permanent	
SEPA Registrations, Licenses and Consents	permanent	
Specifications for work tendered	6 years	
Tenders (successful)		See 'Contracts' above
Tenders (unsuccessful)	6 years	
Waste Consignment Notes- Controlled wastes such as clinical/ healthcare and household/ domestic	2 years	
Waste Consignment Notes- Special/ Hazardous/ Radioactive Wastes	3 years	
Waste- Duty of Care Inspection Reports	permanent, or for life of external contract	

## Administrative Records - Human Resource

<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Disciplinary: First written warning	6 months	
Disciplinary: Final written warning	12 months	
Disciplinary: First and final written warning	12 months	
Disciplinary: Letter of Dismissal	10 years	Where action is in prospect or has been commenced, consult with legal representatives and keep in accordance with advice provided.
Disciplinary: Records of action taken, including: Details of rules breached, Employee's defence or mitigation, Action taken and reasons for it, Details of appeal and any subsequent developments	6 years after leaving service	See above for retention periods for warnings.
Establishment records - major (including: Personnel files, letters of application and appointment, confirmation of qualifications, contracts, joining forms, references & related correspondence, termination forms)	6 years after leaving service	

<b>Human Resources Records</b>		
<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Establishment records - minor (including: attendance books, annual leave records, duty rosters, clock cards, timesheets)	2 years	
Industrial relations (not routine)	permanent	
Personal Development: Nurses - training records	30 years after completion of training	Applies only to Nurse Training carried out in hospital based nurse training schools
Personal Development: Study leave applications	2 years	
Recruitment: Applications for employment- unsuccessful applicants	1 year after completion of recruitment procedure	
Recruitment: CVs for non-executive directors (successful)	5 years following end of term of office	
Recruitment: CVs for non-executive directors (unsuccessful applicants)	2 years	
Recruitment: Disclosure Scotland information	90 days	90 days after the date on which recruitment or other relevant decisions have been taken; or 90 days after the date on which recruitment or other relevant decisions have been taken.
Recruitment: Job advertisements	1 year	



## Administrative Records - Procurement and Stores

<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Approval files - contracts	permanent	
Approved suppliers lists	11 years	
Delivery notes	2 years	
Indents	2 years after financial year referred to	
Medical equipment specifications - major items purchased	permanent	
Medical Equipment-operating manuals	operational lifetime of equipment	
Procurement documentation	7 years	One copy of each supplier response from short listed to tender and the contract itself.
Products - liability	11 years	
Purchase orders	3 years after financial year referred to	
Requisitions	2 years after financial year referred to	
Stock control reports	2 years	
Stores - major (ledgers etc.)	6 years	
Stores - minor (requisitions, issue notes, transfer vouchers, goods received books etc.)	2 years	

<b>Procurement and Stores</b>		
<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Supplier correspondence	6 years after termination of agreement	
Supplies records - minor (e.g. invitations to tender and inadmissible tenders, routine papers relating to catering and demands for furniture, equipment, stationery and other supplies)	2 years	

## Administrative Records - NHS Board

<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Area health plans	permanent	
Contracts - non sealed on termination	6 years	
Contracts- GP Practices and others to deliver core NHS services	permanent	
Contracts – sealed	permanent	Including associated records
Corporate policies	permanent	
Deeds of title	permanent	
Health promotion – core papers and visual materials relating to major initiatives	consider permanent preservation	
History of Boards or their predecessor organisations	permanent	
History of hospitals	permanent	
Hospital services files	consider permanent preservation	
Legal actions (adult)	7 years after case settled or dropped	
Legal actions (child)	until child is 18 or 7 years after case settled or dropped, whichever is later	
Litigation dossiers - complaints including accident reports	10 years	Where a legal action has commenced see Legal actions

<b>NHS Board Records</b>		
<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Meeting papers - master set	permanent	Main committees and sub-committees of NHS Boards and special Health Boards and other meetings of significance for legal, administrative or historical reasons
Minutes - master set	permanent	Main committees and sub-committees of NHS Boards and special Health Boards
NHS circulars - master set	permanent	
Nursing homes pre 1 April 2002: registration documents and building plans	permanent	The regulation of care services was taken over by the Care Commission on 1st April 2002.
Nursing homes pre 1 April 2002: inspection reports and general correspondence	5 years	The regulation of care services was taken over by the Care Commission on 1st April 2002.
Option appraisals	6 years after end of agreement	
Patient complaints without litigation -adults	7 years	
Patient complaints without litigation – children and young adults	until child is 16 or 7 years, whichever is later	

<b>NHS Board Records</b>		
<b>TYPE/ SUBTYPE OF RECORDS</b>	<b>MINIMUM RETENTION PERIODS</b>	<b>NOTES</b>
Photographs	consider for permanent preservation	Corporate and publicity photographs, not used those for patient care purposes.
Press cuttings	consider for permanent preservation	
Register of seals	permanent	
Reports - major	permanent	
Serious incident files	permanent	
Service development reports	6 years	
Service level agreements	6 years	
Strategic plans	permanent	
Subject files	permanent	Files relating directly to the formulation of policy and major controversies must be permanently preserved. Other files should be disposed of when no longer needed.
Trust arrangements legally administered by NHS organisations - documents describing terms of foundation/ establishment and winding-up	permanent	
Trusts arrangements legally administered by NHS organisations - other documents	6 years	

## Administrative Records - Service Planning

<b><i>TYPE/ SUBTYPE OF RECORDS</i></b>	<b><i>MINIMUM RETENTION PERIODS</i></b>	<b><i>NOTES</i></b>
Activity monitoring reports	6 years after end of agreement	
Admission, transfer and treatment of patients- policy files	permanent	
Databases - demographic and epidemiological based on data supplied by NHS National Service Scotland, Information Services		In accordance with general policies of NHS National Service Scotland, Information Services, and any specific terms and conditions imposed by them in relation to particular data sets
Databases - demographic and epidemiological based on survey data		May be retained indefinitely if data quality and potential for future re-use justifies cost of migration / regeneration to new formats and platforms
Patient activity data	3 years	
Summary bed statistics	permanent	
Waiting list monitoring reports	6 years	
Winter business plans	6 years	