SCOTTISH GOVERNMENT RECORDS MANAGEMENT

HEALTH AND SOCIAL CARE CODE OF PRACTICE (SCOTLAND) 2020

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.

The Scottish Government, Edinburgh 2020

This document is available from the Scottish Government Health and Care Information Governance website at https://www.informationgovernance.scot.nhs.uk/

The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

Produced by the Scottish Government supported by the National NHS Scotland Records Management Group.

Published by the Scottish Government, June 2020

DOCUMENT CONTROL SHEET

Title:	Records Management: Health and Social Care Code of Practice
Date Issued:	18th May 2020
Effective From:	1 June 2020
Version/Issue Number:	202006
Document Type:	Code of Practice
Document status:	Active
Author:	Scottish Government lead Short Life Working Group for the RM CoP review Contacts: Elena Beratarbide, IG Policy Lead, Information Assurance & Governance Team, NHS Scotland, Health and Social Care DHCIG@gov.scot Tracy Gill, Chair NHSScotland Records Management Group.
Owner:	Scottish Government, Digital Health and Care Directorate
Contact:	DHCIG@gov.scott
Target Audience	Records Managers, Information Governance Leads, Data Protection Officers, Caldicott Guardians, Senior Information Risk Owners – with responsibility to cascade to all staff
Supersedes	Scottish Government Records Management: NHS Code of Practice (Scotland) Version 2.1 January 2012

Distribution list : open access to this document is available via the NHS Scotland IG website publications: https://www.informationgovernance.scot.nhs.uk

Contents

SECTION 1 - **Foreword**

1.1 Background

1 The Records Management: NHS Code of Practice, version 2.1, was published by the Scottish Government in January 2012, 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.

2 This document is a refreshed version for a wider setting including Health and Social Care. It is based on current legal requirements and professional best practice.

3 This guidance has been drafted by the Scottish Government in collaboration with representatives of the Scottish Health and Social Care setting, including records managers, archivists and information governance experts from the NHS, Local Authorities and GP Practices.

4 This 2019 update specifically takes into account the Public Records (Scotland) Act 2011, the Public Bodies (Joint Working) (Scotland) Act 2014, the Children and Young People (Scotland) Act 2014, the Multi Agency Public Protection Arrangements (MAPPA), the Health Board Provision of Healthcare in Prisons (Scotland) Directions and recommendations for Records Management from key recent public inquiries, particularly the Scottish (Historical) Child Abuse Inquiry (2015). This review also takes in the requirements of recent changes to the following:

- Data Protection legislation[1],
- NHSS Information Security Policy Framework (2018 and 2019) [2]
- and the extended powers of the Information Commissioner's Office (ICO)[3],

5 It's recognised that the culture within the health and social care context is changing as a result of greater service integration driven by the Digital Health and Care Strategy 2018. Together with the natural evolution towards a digital paper lite environment, and the use of portals for health and social care groups, clinicians and patients. This Records Management for Health and Social Care

1 General Data Protection Regulation (EU) 2016/679 ("GDPR")
[2] Scottish Government and 2019 Framework 2018 Information Security Policy Framework and 2019 Framework
[3] Information Commissioner's Officer (ICO)

Code of Practice 2019 (from this point onwards referred to as the Code of Practice) is a guide to the practice of managing records. It is relevant to organisations who work within, or under contract to NHS organisations in Scotland. This also includes public health functions in Local Authorities and Social Care where there is joint care provided within the NHS.

6 This Code of Practice forms part of a series of information governance and security guidance, including those published by the Scottish Government, and consulted with the following organisations:

- British Medical Association (BMA);
- General Medical Council (GMC);
- Information Commissioner's Office (ICO)

1.2 Strategic Context

7 The Digital Health and Care Strategy 2018 is ambitious; to create a digital and interoperable health and social care system, supporting improvement in safety, effectiveness, efficiency and citizen-centred nature of the services we offer.[4]

8 The strategy focuses on digital innovations for which this Code of Practice plays an important role; this Code of Practice is a guide on how to manage those records within such technologies to enable communication, integrate care, enhance availability of information and better working practices.

9 This Code of Practice is one of many actions brought forward from the NHSS Information Security Policy Framework 2015/17 to ensure the confidentiality, integrity and availability of NHSS information and that it is processed in a fair and lawful manner.

10 Information and communication technologies are important to the progress and the ambitions set out in The Healthcare Quality Strategy for NHS Scotland 2010 to actively support and enable quality improvements in healthcare services across Scotland.

11 In this strategic context, the Code of Practice is key to ensure a comprehensive NHS health and social care record is available at the point of need in Scotland. The success of this will depend on many factors, some of them out with this code of practice. Other workstreams from the Digital Health and Care Strategy 2018, and good records management will be essential to ensure paper and electronic records are managed consistently.

[4] Scotland's Digital Health & Care Strategy 2018

1.3 Aims

12 This Code of Practice aims to:

- establish records management best practice in relation to the creation, use, storage, management and disposal of NHS records (including, where appropriate, the archival preservation 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 and security standards;
- set out recommended periods of retention for NHS personal health records and administrative records and social care records held by NHS Boards, regardless of the media on which they are held; and
- indicate where further information on records management may be found;
- explain the requirement to select, and transfer to an archive service, those records for archival preservation.

13 This is an evolving document because standards and practice covered by the Code of Practice will change over time. It will be subject to regular reviews and updated as necessary, with the next review scheduled for 2021.

1.4 Types of Records Covered by the Code of Practice

14 This Code of Practice applies to NHS records in any format (e.g. paper, electronic, microfilm, audio, SMS, etc.), including those handled by third parties on behalf of the NHS either in connection with health and social care, corporate or administrative purposes. Record formats include:

- E-mails
- social media (social media includes blogs, wikis and social networks, for example Twitter, Facebook and Skype)
- website content (internet or intranet)
- voice recording

15 A record is “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". (ISO 15489-1:2016 *Information and documentation - Records management*.[5]) This definition extends to the archive role, particularly in recording corporate memory.

16 A health record 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.

17 The following are examples of records covered by this Code of Practice:

- personal health records (paper based or electronic including those concerning all specialties, and GP medical records);
- records of clinical trials;
- records of private patients seen on NHS premises;
- records of blood and tissue donors;
- accident and emergency, birth, and all other registers;
- theatre registers and minor operations (and other related);
- x-ray and imaging reports, output and images, film/video;
- administrative records (including, for example, staff, complaints, financial, property, environmental, health and safety, human resource, procurement/stores, NHS Board and service planning records). Also includes data processed for purposes other than direct care (secondary purposes), including planning and management of services and research;
- health records shared with or transferred to other services (e.g. prisons, integrated health and social services, education and public protection agencies)

18 Any organisation that processes NHS data under the Scottish Health and Social Care Integration Scheme should use this Code of Practice, including subcontractors processing data on behalf Public Bodies in Scotland.

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

SECTION 2 - **Introduction**

19 This Code of Practice draws on advice and published guidance available from the Scottish Government Freedom of Information Unit and the National Records of Scotland, and from best practice 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 and security workstreams.

2.1 General Context

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

21 All NHS organisations, Local Authorities and Integrated Joint Boards involved in either health or social care, are public authorities under Schedule 1 of the Freedom of Information (Scotland) Act 2002 (FOISA), and the records they create are subject to the Public Records (Scotland) Act 2011 (PRSA). These organisations and the Scottish Ministers are obliged under Data Protection, Freedom of Information, and the Environmental Information Regulations, to make arrangements for the safe keeping and eventual disposal including transfer to an archive of all types of records. This Code of Practice is based on the Scottish Government's understanding of the relevant law in Scotland, 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 that arise regarding the matters covered in this Code of Practice.

22 Where a local authority is in partnership with an NHS Board in Scotland for the provision of Integrated Health and Social Care services, the local authority must manage the associated Health and Social Care public records in accordance with the requirement to make proper arrangements under Section 53 of the Local Government etc. (Scotland) Act 1994.

23 Organisations that are not bound by the PRSA or the Local Government etc (Scotland) Act 1994 may have a contractual requirement to manage records on behalf of the NHS, a local authority or an Integrated Joint Board (e.g. as part of an NHS Standard Contract).

24 FOISA and the Data Protection Act (DPA) 2018 have guidance on records management practice that recommend the systems and policies that must be in place to comply with the law.

25 Organisations have 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 after an employee or contractor has left the NHS. Obligations around confidentiality remain even after the death of a patient.

26 Other legislation requires information to be held as proof of an activity against the eventuality of a claim (e.g. Limitation Act 1980 or the Consumer Protection Act 1987).

27 Records are a valuable resource because of the information they contain. High quality information underpins the delivery of first-class evidence-based health and social 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:

- support integrated health and social care;
- support day to day business which underpins the delivery of care;
- support evidence-based clinical and social care practice;
- support sound administrative and managerial decision making, as part of the knowledge base for health and social care services;
- meet legal requirements, including requests from patients and customers or other individuals made through provisions of FOISA or Data Protection legislations;
- assist clinical and other audits;
- support improvements in health and social care effectiveness through research;
- 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 them.

28 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 Principles in the

GDPR) 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.

29 All individuals who work for an NHS organisation or local authority are responsible for any records that they create or use in the performance of their duties.

2.2 Regulatory Framework: Legal and Professional Obligations

30 The principal legislation governing the management of records is PRSA. The Act places an obligation on public authorities to prepare and implement a records management plan which sets out proper arrangements for the management of their records.

31 Any record that an individual creates is subject to PRSA, and the information contained in such records is subject to FOISA and Environmental Information (Scotland) Regulations 2004 (EIR). There is a specific requirement under Regulation 4 on a public authority to take reasonable steps to organise and keep up to date environmental information relevant to its functions. The GDPR and DPA 2018 are the principal legislations governing how organisations process and handle personal identifiable information. They set in law how personal and special category personal information may be processed.

The data processing principles are:

a. processed lawfully, fairly and in a transparent manner;

b. collected for specified, explicit and legitimate purposes;

c. adequate, relevant and limited to what is necessary;

d. accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;

f. processed in a manner that ensures appropriate security of the personal data.

32 FOISA was designed to create transparency in Government and allow any citizen to know about the provision of public services through the right to submit a request for information. This right is only as good as the ability of those organisations to supply information through best practice records management

programmes. Records managers are required to adhere to a Code of Practice issued under Section 61 of FOISA.

33 Further information on legal and professional obligations is available on the Scottish Government Information Governance website www.informationgovernance.scot.nhs.uk

2.3 Social Care Records

34 This Code of Practice refers to health and social care records that are held by an NHS Board, including those used in the provision of integrated health and social care services. For those health and social care records that are held at local authority level, they will fall under the scope the Scottish Council on Archives Record Retention Schedules (SCARRS).

35 NOTE: Shared social care and authority records should be held for the longest retention period specified in the Code of Practice or SCARRS.

SECTION 3 - **Roles and Responsibilities**

36 Effective records management enables Health and Social Care organisations to provide and maintain a high level of service to the public. Adherence to this Code of Practice will support organisations to act in accordance with legal requirements, standards, evidence-based practice and professional work practice.

37 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, throughout their lifecycle, from planning and creation through to ultimate disposal. It should have clearly defined responsibilities and objectives, and necessary resources to achieve them.

38 **The NHS Board and the Local Authority** are responsible for ensuring they meet their legal responsibilities.

39 **The Integrated Joint Board** is responsible, by delegation of their corresponding NHS Board and local authority, for ensuring there are suitable arrangements across the integrated services to meet the legal responsibilities of the partners, and for the adoption of the agreed governance arrangements.

3.1 Roles

40 **The Chief Executive of the NHS Board/Local Authority** has overall independent responsibility for records management in their organisation and joint responsibility across the Health and Social Care Partnership(s). As accountable officer they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. This overall responsibility is delegated to the **Senior Information Risk Owner (SIRO)**.

41 **The Senior Information Risk Owner (SIRO)** has responsibility for ensuring information assets (including records) are processed in a safe, fair and lawful manner, regardless of whether the information is processed using digital technologies or not.

42 **The Caldicott Guardian** has responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring use of patient identifiable information is legal, ethical and appropriate, and that confidentiality is maintained.

43 **The Data Protection Officer (DPO)** role and responsibilities are defined in Section 4 of the EU General Data Protection Regulation 2016. Article 39 sets out key tasks all DPOs must undertake as part of their role. This includes:

- informing and advising the controller or the processor, and their employees, of their obligations under data protection legislation;
- monitoring the implementation and application of the organisation's policies and training on data (information and records) management as well as monitoring the application of these policies;
- providing advice, where required, on data protection impact assessments and monitor compliance with this requirement;
- act as point of contact for the ICO for any matter relating to the data protection legislation and to co-operate with the ICO as required;
- to keep documentation on at least the name of the data flows, the purpose of the processing, the types of subjects and data, the security and privacy risks and the time limits for data erasure (according to Article 30). Likewise, they must monitor personal data breaches and responses to the supervisory authority (ICO).

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

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

46 **The Archivists** are responsible for collecting, cataloguing, preserving and managing appropriate access to valuable historical information. Archivists liaise with records managers, data protection officers and other information governance professionals to train and identify relevant material of historical value ensuring transfer to archival preservation. Note that valuable historical information may be 'born digital' and exist as electronic files as well as traditional paper archives.

47 **All NHS staff**, whether clinical or administrative, who create, receive and use documents and records have records management responsibilities. All staff should ensure that they keep appropriate records of their work and manage those records in keeping with the Code of Practice and the relevant policies and guidance within their Board. NHS managers should demonstrate active progress in enabling staff to conform to the Code of Practice, identifying resource requirements and any related areas where organisational or systems changes are required.

3.2 Training

48 All staff within the NHS Board or its partners involved in handling records on behalf of the NHS, whether clinical or administrative, should be appropriately trained in their records management responsibilities, and are competent to carry out their designated records management duties. Training should include both paper and electronic record formats.

49 NHS Boards have a duty to ensure the provision of training for staff regarding records management in support of their compliance with Element 12 of their Records Management plan (RMP), under PRSA. Specific elements should be included in training programmes to ensure staff understand appraisal and retention of records.

3.3 Policy and Strategy

50 In support of their compliance with Element 3 of their RMP, each NHS Board should have in place an overall records management policy statement, endorsed by the Executive Management Team (or its equivalent) and made readily available to staff at all levels of the NHS Board.

51 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.

52 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 procedures 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 lifecycle, from their creation, usage, maintenance and storage to their disposal be it ultimate destruction or archival preservation;

- provide a framework for supporting standards, procedures and guidelines;

- indicate the way in which compliance with the policy and its supporting standards, procedures and guidelines will be monitored and maintained.

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

SECTION 4 - NHS Records Management and Information Lifecycle

54 PRSA requires every authority to prepare a “Records Management Plan” setting out proper arrangements for the management of their public records throughout their lifecycle.

55 Records (and the information in them) are considered to have a "lifecycle". This “lifecycle” starts at creation or receipt of the record in the organisation and continues throughout the period of its 'active' use, then into the period of 'inactive' retention (such as closed files which may still be required occasionally for reference purposes). The “lifecycle” concludes with either confidential disposal or (for a very small proportion) archival preservation in an archival facility as designated in the RMP.

56 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 or retained by archive.

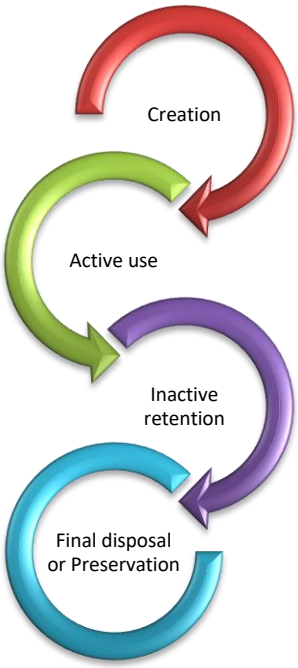

Figure 1 The Information (Records) lifecycle

57 The ISO 15489:2016 Information and Documentation - Records Management Standard focuses on the business principles behind records management and how organisations can establish a framework to enable a comprehensive records management programme.

58 The standard describes the characteristics of a record (authenticity, reliability, integrity and usability). These characteristics allow strategies, policies and procedures to be established that will enable records to be authentic, reliable, integral and usable throughout their lifecycle.

59 To ensure that these characteristics are maintained, sufficient persistent metadata must be attached to each record. It is essential that a records management process is designed that will allow records to possess these characteristics.

60 The industry standard for the design and implementation of records management, as given in the ISO standard ISO15489-1:2016, is an eight-stage process that can be summarised as follows.

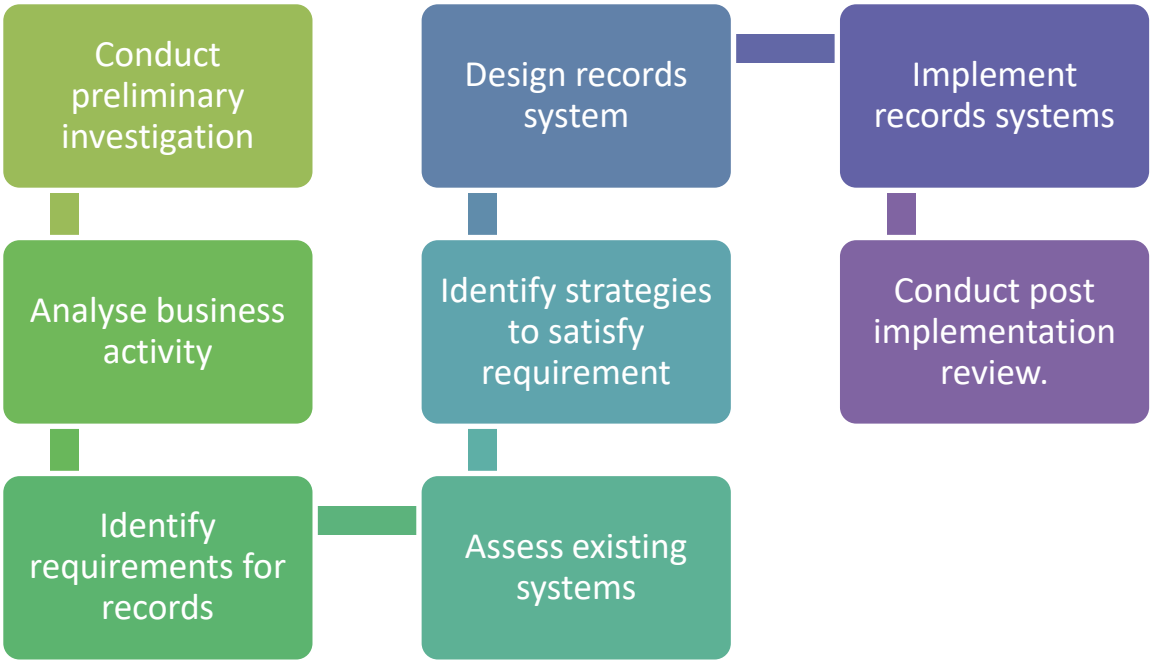

Figure 2 Implementation of records keeping process. Further details can be sought from the ISO standard and supplementary guidance.

61 In addition to the stages outlined above, in most cases an information risk assessment should also be conducted.

62 The risk assessment should include identified privacy risks in compliance with the ICO Data Protection Impact Assessment Guidelines.

4.1 Records Creation

63 Each organisational unit (for example Finance, Estates and Facilities, eHealth, Human Resources, Direct Patient Care, Health & Social Care integrated services) of an NHS organisation should have in place procedures for documenting its activities. This process should consider the legislative and regulatory environment in which the unit operates.

64 Records of organisational activities should be complete and accurate in order to:

- to allow employees 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;
- to ensure authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.

65 Appropriate version control arrangements that support the management of multiple revisions to the same document should be in place.

66 Records created by the NHS (or on its behalf) 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 frameworks.

67 Not all documents created or received by NHS employees in the course of their work need to be retained for any period of time. For example, some emails are of only passing value and can be deleted as soon as they have been read or actioned. However, emails containing significant information or instructions should be retained, as appropriate, within the record-keeping system. It should be recognised that the decision to dispose of these records immediately is still made within the context of the overall record-keeping system.

68 When creating a new type of record, an initial IRA (Information Risk Assessment) must be conducted in conjunction with those responsible for information security and data protection. The Information Asset Owner is responsible for conducting the IRA. Any new information asset (e.g. a new type of record) containing NHS health or corporate records must be “declared” or “registered” with the corresponding NHS Data Protection Officer.

4.2 Managing Records

69 Implementing and maintaining an effective records management system 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 etc.). An information survey or record audit is essential to meet this requirement. The survey will provide a description of the record collection along with its location

and details of the responsible manager. This ensures control over the records and provides valuable data for developing records appraisal and disposal policies and procedures.

70 Paper and electronic record management 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.

71 The record management system, whether digital or not (e.g. paper or microfiche), should include a documented set of rules for document labelling and 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.

72 Records should be structured within an organisation-wide corporate "file plan" (Business Classification Scheme and/or Information Asset Register) which reflects the functions and activities of the organisation and facilitates the appropriate sharing and effective retrieval of information.

73 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 at https://ec.europa.eu/ldabc/en/document/2303/5927.html

74 Where an EDRMS is not yet available, electronic records should be stored on shared, network servers in a clear and meaningful folder structure. The folder structure should reflect the organisation's file plan (Business Classification Scheme and/or Information Asset Register) in the same way as paper files, which represent the functions and activities of the organisation. The server should be subject to frequent back-up procedures in line with the NHS Scotland Information Security Policy Framework (2018)[6]. Users should apply the functionality of the relevant software to protect electronic documents against inappropriate amendment. Please note: it is almost impossible to fully protect documents in a non EDRMS environment or provide full audit and authenticity evidence.

4.3 Records Maintenance - Storage and Scanning

75 Organisations storing or scanning NHS records should put in place robust procedures to manage control of access, retrieval and use of records to ensure

[66] 2018 NHS Scotland Information Security Policy Framework

continued integrity, reliability and authenticity of the records as well as their accessibility for the duration of their retention including the time of their disposal or archival preservation.

76 NHS organisations may consider the option of scanning records which currently exist in paper format into electronic format, for reasons such as business efficiency.

77 It is vital to highlight the importance of actively managing records which are stored in offsite storage (paper or electronic). This will ensure that the organisation maintains a full inventory of what is held offsite, retention periods are applied to each record, a disposal log is kept, and security risk assessments (including privacy impact) are conducted on provided handling data/records offsite.

4.4 Records Inventory/Information Asset Register

78 Each NHS organisation should 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.

4.5 Records Management Systems Audit

79 The NHS organisation will regularly audit its records management practices as part of its existing audit activity. This can include checking for adherence with this Code of Practice. Results of audits will be reported to the NHS Board through the appropriate committee.

80 This audit must be extended to integrated Health & Social Care services handling health and corporate records as applicable.

4.6 Disclosure and Transfer of Records

81 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 section 2.2 (Regulatory Framework: Legal and Professional Obligations).

82 The mechanisms for transferring records from one organisation to another should also be tailored to the sensitivity of the material contained within them and the media on which they are held.

83 Data Protection Officers and Caldicott Guardians must be able to advise on the appropriateness of disclosing or transferring records which contain personal identifiable information and any requirement for gathering further authorisation.

84 Information Security staff should be able to advise on appropriate safeguards. The NHS Scotland Information Security Policy Framework and eHealth Mobile Data Protection standard set out the requirements for the safe handling and transmission of corporate and health records, across a range of media.

4.7 Retention and Disposal Arrangements

85 Detailed guidance for retention and disposal of personal health records can be found in Section 6 and 7.

86 It is particularly important 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. In addition, the disposal of records should be clearly documented.

87 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.

88 Each NHS organisation should have a policy which has been written/reviewed within the last three years, for the retention, archiving or destruction of the organisation's records in accordance with the PRSA. 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 policy 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.

89 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.

4.8 Appraisal of Records

90 Appraisal refers to the process of determining whether records require to be either retained for longer, destroyed as they have reached the end of their retention period or are worthy of archival preservation. This can be undertaken

in consultation with an NHS Health Board Archivist, an Archivist from the Board's named place of deposit (as identified for Element 7 of RMP) or the National Records of Scotland.

91 This is a compulsory element under the terms of the Public Records (Scotland) Act 2011 Section 1 2(b)(iii).

92 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 for archival preservation. In addition, samples of health records 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.

93 Health and Social Care Case records, including complaints, which meet the following criteria should also be considered for archival preservation (Note: this is not an exhaustive list and there may be other record types that would fall into this category):

- National public interest
- A change to policy or procedure for delivery of care
- Regulatory action or records that document decision-making at a senior level
- Sustained media attention
- Serious case reviews e.g. published reports, records created and received in the course of implementing recommendations of serious case reviews.
- Records relating to any inquiry conducted under the Inquiries Act

94 In line with the obligation placed upon the Keeper of the Records of Scotland (The Keeper) under PRSA, the National Records of Scotland has issued general guidance regarding public authorities archiving policies and transfer arrangements. This is accessible via www.nrscotland.gov.uk Model Plan Guidance to Element 7.

95 It is expected that only a small proportion of records will require archival preservation, however, appraisal before disposal is essential. For these purposes NHS Boards should have procedures and staff guidelines in place,

written in consultation with the archivist from the repository named in element 7 of the RMP.

4.9 Records Closure

96 Records should be closed (i.e. made inactive and appraised for archival preservation) as soon as they have ceased to be in active use. 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.

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

4.10 Records Disposal

98 Organisations should have a retention/disposal policy that is based on the retention schedules referred to in this Code of Practice. The policy should be supported by, or linked to, the retention schedules, which should cover all records created. 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 Section 6 and 7 of this Code of Practice, for the organisation.

99 Records selected for archival preservation and no longer in regular use by the organisation should be transferred to an archive once the business need has expired.

100 Best practice suggests that non-active records selected for archival preservation should be transferred no later than 30 years from creation of the record, with electronic records being transferred within a shorter period.

101 Records (including copies) not selected for archival preservation and which have reached the end of their administrative life should be destroyed in a secure manner 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 BSEN 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 after an employee or contractor has left the NHS. Obligations around confidentiality remain even after the death of a patient.

102 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.

103 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:

- 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);
- disposal schedules would constitute the basis of such a record.

104 Whenever health 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 present to the service or make a Subject Access Request.

105 Personal health records should not be destroyed before the end of the period stated in the Code of Practice Section 6 and 7. These periods reflect the statutory time limits for legal action to be taken.

106 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 (FOISA) have been exhausted or the legal process completed. It is important to note that section 65 of FOISA and Regulation 19 of the Environmental Information (Scotland) Regulations 2004 provide that it is a criminal offence to destroy records with the intent to prevent disclosure.

107 Data Protection legislation requires the data controller to retain personal data no longer than is necessary for the purpose the information was obtained for. Ensuring personal data is disposed of when no longer needed will reduce the risk that it will become inaccurate, out of date or irrelevant.

108 In complex settings where the information is shared across different parties, the retention period should be consistent across all parties. Retention periods should be aligned to the data controller's retention periods.

4.11 Records Security and Business Continuity

109 The 6th Data Protection Principle requires organisations to take reasonable technical and organisational security measures to protect information from unauthorised access, unlawful processing, accidental loss, destruction or damage.

110 The NHSS Information Security Policy Framework (2018) requires NHS Boards to work as closely as possible to ISO27001 in order to ensure best practice security and business continuity is in place. ISO 27001 is a specification for an information security management system (ISMS).

SECTION 5 - **Useful Guidance**

111 In this section you can find additional guidelines for dealing with a number of issues raised.

5.1 Adopted Persons Health Records

112 Records must be recorded under birth names (or alternatively an alias) until an adoption order is granted.

113 This type of record is subject to a high risk of unauthorised disclosure of personal details, especially in relation to third parties, therefore it is recommended that redaction and disclosure instructions are clearly stated along with the record.

114 Any new records derived from the original records of the adopted person must contain sufficient information to allow for a continuity of care.

115 GPs must initiate any changes of CHI number or identity if it is considered appropriate to do so, following the adoption.

5.2 Ambulance Service Records

116 Ambulance service records must be considered as health records if they contain medical evidence (e.g. clinical interventions), and therefore subject to the same retention periods as their corresponding health records (e.g. adult, children etc.).

117 If Ambulance service records do not contain health data (or data that's clinical in nature) they must be treated as administrative records (e.g. a patient transport record with no clinical details).

118 The sharing of records between the ambulance service and any organisation part of the wider NHSS (and partners) must be documented in a corresponding Information Sharing Agreement (e.g. National Intra NHS ISA). Suitable work instruction must be written at local level as required e.g. to ensure the ambulance service can access original handover records if needed, to share information with drugs, alcohol and substance misuse teams etc.

5.3 NHS 24 Records

119 The sharing of records between NHS 24 and any organisation which is part of the wider NHSS (and partners) should be documented in a corresponding Information Sharing Agreement (e.g. National Intra ISA) and suitable work instructions must be written at local level as required.

5.4 Asylum Seeker Records

120 Records for refugees and asylum seekers must be treated in exactly the same way as other health records. CHI numbers must be allocated. In addition to the electronic record, refugees and asylum seekers should be given an eligibility card to help them register if they move to another part of Scotland. Their patient records are maintained on the NHS systems and although they can request copies of their records if they wish but, handheld records are not the standard.

121 If a refugee or asylum seeker arrives with a handheld record, this should be used to help populate their NHS Scotland medical record and to create an emergency care summary. The handheld record should be considered similar to an emergency care summary/anticipatory care plan, updated after the patient is seen and returned to the patient.

5.5 Child School Health Records

122 Health records held by school or school nurses must be individual in nature (one record per child) in order to allow independent processing in line with the Data Protection Act 2018.

123 Schools may process some health data on behalf of a Health Board, in which case they must follow work instructions for the data controller (the Health Board or the organisation who hold the statutory obligation to provide the service for which the information is collected e.g. NHS vaccination or dental programmes). The health care public function for which these records are processed is assigned to the Health Board where the child resides, regardless where the school that is processing data on their behalf is located (e.g. within or out with the NHS Board territorial area).

124 Schools (local authorities, education department) are the Data Controller for Health records held at school for the school own purposes (e.g. as part of Integrated Support Plans).

125 Health records processed on behalf of the Health Board, when stored on a school premises, must have access restricted to the health staff delivering care unless there is another lawful basis to access the record.

126 Health and Social Care partnerships must include in their information sharing agreements, suitable work instructions to cover processing, how data will be collected, transferred to school nurses and/or child dental services, kept up to date etc.). These records are subject to the retention periods in this Code of Practice regardless of where they are stored.

5.6 Complaints Records

127 Complaint information, including clinical opinions about the care that was delivered should never be recorded in the health records, particularly if the complaint is unfounded.

128 Any single complaint must be contained in a single record, regardless of the number of teams involved in the investigation/handling. This will allow a holistic view of the complaint and easier access to the record.

129 Complaint records must follow the NHS Scotland Complaints Handling Procedure.

5.7 Controlled Drugs Regime

130 Refer to NICE[7] guideline [NG46] (2016) for "Controlled drugs: safe use and management". They have specific guidelines for record keeping, controlled drugs registers, requisitions, record of destruction and invoices, standard requisition forms, risk assessment records etc.

131 Further information can be found on the Healthcare Improvement Scotland (HIS) website on the 'safe management and use of controlled drugs.[8]

5.8 Data Processors, Subcontractors and Changes in Contracts

132 Subcontractors processing data (records) on behalf of health and/or social care organisations must abide by this Code of Practice.

133 Subcontractors have a liability beyond the end of the contract to retain records until the period of liability has expired. Contracts and relationships with third parties must be managed so that other aspects of records management (and its information) are protected. This includes data protection clauses, returning the data or transferring the data to a new supplier to ensure continuity of service.

134 Data Protection Officers should be consulted and advise when additional fair processing notices are required.

135 Records stored offsite, particularly at subcontractors' premises, should be included in the Information Asset Register of the health and/or social care organisation. They are subject to regular monitoring, including at contract reviews as part of healthy supplier relationship management.

---

[7] National Institute for Health and Care Excellence.
https://www.nice.org.uk/guidance/ng46/chapter/recommendations

[8] http://www.healthcareimprovementscotland.org/our_work/governance_and_assurance/controlled_drugs/controlled_drugs_report.aspx

136 Should a subcontractor's closure or cease business, a plan to transfer the records to a suitable authority must be put in place, this includes the closure of a GP Practice.

5.9 Deceased Person

137 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;
- death certificates;
- where a person has a right of access under the Access to Health Records Act 1990;
- whether the information is already in the public domain. The purpose of the disclosure and any benefit or harm that will accrue as a result;
- individuals close to the deceased.

138 The Freedom of Information (Scotland) Act 2002 confers a right of access to a 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.

139 The Access to Health Records Act 1990 governs access to records of a deceased person. It applies only to records created since 1 November 1991. Access must also be given to information recorded before these dates if this is necessary to make any later part of the records intelligible. The Act allows access to:

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

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

141 In certain circumstances, such as a request for medical records of the deceased, the exemption for confidential information is likely to apply. Public authorities must conduct a test of confidentiality prior to disclosure (refer to ICO guidelines "Information provided in confidence" for further details on this test).

142 As with the Data Protection Act 2018, a medical professional or the data controller may be required to screen and redact the notes before release as, on occasion, information about the deceased will contain information about other living individuals, including genetic information that may identify surviving relatives (personal identifiable data under Data Protection Act 2018).

143 In the case of information about the deceased that is environmental in nature, the Environmental Information (Scotland) Regulations (EIRs) will apply. Where information about the deceased is subject to the EIRs, public authorities should in most cases consider regulation 10(5)(f) as the 'equivalent' to section 36 of FOISA.

144 Individual cases will always be decided on the basis of their particular circumstances.

145 Organisations should have processes that address where and how the records of deceased persons are stored. Secure 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 legislation.

146 Section 6 contains specific provision for the retention of records relating to deceased individuals, in particular:

- cell/tissue transplantation including donated organs from deceased individuals;
- for autopsy reports, specimens etc. where the deceased has been the subject of a Procurator Fiscal autopsy.

5.10 Digital Records

147 Managing electronic records presents a significant challenge, especially for typical health and social care organisations, where electronic records are stored in a large variety of databases, email and file systems (including shared drives), which have no standardisation in place. The risk of alteration or deletion makes this challenge even greater.

148 The paper records management system in place in most health and social care organisations, is not necessarily appropriate as the model for managing electronic records. This is because of the nature and volume of electronic records, the variety of file formats, the distribution of the storage and duplication (e.g. parallel datasets) and the way it is backed up and preserved, and the difficulty to implement retention policies unless embedded in the initial digital infrastructure.

149 Electronic records management needs to be very carefully considered and structured to ensure the integrity of the records is not compromised upon capture and data remains for as long as it is required.

150 Where the electronic system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain demonstrating that a record has been destroyed, then the Code of Practice should be followed in the same way for electronic records as for paper records.

If the system does not have this capacity, then once the records have reached the end of their retention periods, they should be made inaccessible to users of the system and upon decommissioning the system (along with audit trails) should be retained for the retention period of the last entry related to the schedule.

5.10.1 Management of Metadata

151 Metadata is ‘data about the data’ and is used to provide information about electronic records such as creation date, retention period, historical value etc. Health and social care organisations must ensure metadata is included by design when deploying new digital solutions, in order to facilitate the management of electronic records and therefore compliance with current legislation (e.g. Data Protection Act 2018, retention periods).

152 When possible, systems will be configured so that when a user captures a record they are presented with the ‘Properties’ view for the record, a visual prompt for the user to enter some meaningful metadata that can be used to

manage the records. In practice this process cannot be mandated, and users can still enter meaningless information or none if they so choose.

5.10.2 Naming Conventions

153 Health and social care organisations must have guidance for naming conventions of electronic records (files and folders); this helps identify records and folders using common terms and titles. They also enable users to distinguish between similar records to determine a specific record when searching the file system. Naming conventions need not be overly prescriptive or formalised, but they must be clear and well defined. Without naming conventions there is a significant risk of records being destroyed or lost within the file system. Organisations should ensure that sensitive information is never used in the name of a record or folder even where access to the area of the file system is strictly managed. This is to ensure that personal or sensitive data cannot be inferred by casual viewing of a record or folder title.

154 Equivalent conventions must exist for use of “Subject” fields in email systems, adding relevant tags for the classification of the information.

155 Further guidance is available here:

http://www.nationalarchives.gov.uk/documents/information-management/managing-electronic-records-without-an-erms-publication-edition.pdf

5.10.3 Information Asset Registers

156 The General Data Protection Regulation requires organisations to maintain a record of processing activities under its responsibility. This is fulfilled by an Information Asset Register providing it contains details of the information processed by the organisation (electronic or otherwise), the sensitivity and classification, the information risk, groups of users and who the information is shared with. Information Asset Registers can contain details of the correspondent Business Classification Scheme to avoid duplication.

5.10.4 Version Control for Electronic Records

157 In the absence of an ERMS, organisations should include details of the current and previous versions of the record in the metadata and/or using naming conventions for such purpose.

5.10.5 Format on Dates

158 When dates are used in the title/names of electronic files and folders, the organisation must choose a standard format for all users to follow. The most

practical way is the format YYYY-MM-DD or YYMMDD. These formats allow easier searching and sorting.

5.10.6 Access Controls

159 Health and Social Care organisations must have an appropriate access control policy, in compliance with the NHSS Information Security Policy Framework (2018). User access controls include user registration and de-registration, user access provisioning, review of user access rights and the removal or adjustment of access rights. Controls also include the prohibition of shared accounts and access to information based on a need-to-know basis. Organisations must implement, when possible, monitoring systems to allow automated escalation of access misuse to electronic records.

5.10.7 Disposal Management

160 Specific management software may be required to allow automated disposal of electronic records. Retention schedules are defined in Section 6 and 7 of this Code of Practice – the requirement is based on the legal basis for retaining information, hence the format (paper or electronic) is irrelevant. This is a very difficult process and currently represents great challenges for Health and Social Care organisations. Wherever possible, a combination of “disposal by design”, semi-automated monitoring and cleansing, and manual guidelines should be applied to dispose of records according to the records retention schedule.

161 Whilst there is a recognition that efficient disposal management is very difficult using legacy systems, health and social care organisations must demonstrate that disposal management is embedded in their change management process; privacy by design is a requirement for all organisations processing personal identifiable data (GDPR). Failure to demonstrate reasonable steps will constitute a breach of data protection regulations.

5.10.8 Email Management

162 Emails are corporate assets. Organisations must have an email policy with clear rules for managing, storing, deleting and sending/disclosing emails. Failure to manage emails indicates a failing in records management generally. This is a difficult area to manage across all organisations, health and social care organisations should implement special training plans and an audit of working practice to identify and address poor practice. Refer to The National Archives guidance[9] on emails for further details on the management of emails as records

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

and the means of ensuring they are captured and managed so that they are accessible and usable to all relevant parts of the organisation.

163 When emails need to be kept, they must be preserved in their entirety, including any attachments, to protect their integrity.

164 Deletion of emails is an offence under the Freedom of Information (Scotland) Act 2002 and Data Protection Act 2018 once a request for information has been received (e.g. a Freedom of Information request or a Subject Access Request).

165 NHS email accounts are portable across NHS organisations, therefore, in changes of roles or NHS organisations, managers must ensure data is not transferred to the new organisation unless necessary. It will be poor practice to purge email accounts when an individual transfer to another organisation, as some emails may be considered as corporate records, and must be kept where necessary.

166 Emails in relation to patient health care, must be kept with their corresponding health and/or social care record.

5.10.9 Duplication of Electronic Data

167 Where data is duplicated, either due to data warehouses or backup systems, the organisation must be in a position to comply with current legislation, particularly in terms of data quality and accuracy, implementation of rights to deletion, withdrawal of consent for processing personal data and retention schedules across all instances. Information Asset Registers must hold information about data replicated in other systems. Master data management tools must be used where possible to support master data management, removing duplicates and incorporating data rules and standardisation controls to produce an authoritative source of master data. The controls in section 5.11 Duplicate Records are applicable to any record regardless format.

5.10.10 Distributed Records

168 Modern digital records may have very complex and distributed architectures. Nevertheless, the organisation must be able to comply with current legislation, as explained in the above section (duplication of data), regardless how distributed the record is. When the record interlinks with sources of data out with the boundaries of the organisation, arrangements must exist between the information sharing partners to ensure compliance and execution of data subject rights in a smooth manner along the data flow.

5.10.11 Transient Records

169 Within the current health and social care setting there are a range of digital portals. These technologies generate transient records which are still subject to records management, particularly in terms of security measures and access controls. Consideration also needs to be made due to the requirement to evidence decisions made using transient information (particularly when of a sensitive medical or social nature). Logs to show the information available at the time of the record's viewing must exist to evidence what the information contained in any transient records at any point in time, particularly when decisions were made based on such information.

5.10.12 Ownership of Electronic Records

170 Information Asset Registers must record who the Information Asset Owner (IAO) is for any information asset held by an organisation regardless of the format. When new information systems are introduced, the information asset must be registered with the Data Protection Officer and an IAO must be designated. One single system may have more than one information asset with different IAOs, e.g. clinical data vs. operational logs may have different IAOs.

5.10.13 Social Media Records

171 When organisations implement social media channels as a means of communication, they must follow their change management and data protection policies, which must include risk assessment, registration of the information asset, designation of an IAO etc. Appropriate measures should be put in place to ensure compliance with current legislation. Organisations must remember that the data protection legislation has specific exceptions for if the person has made any of their own personal data public via social media channels, however this does not remove the requirement to comply with other regulations such as data subject rights, retention etc.

5.10.14 Scanned Records

172 Providing that the scanning process and procedures are compliant with BSI BIP:0008 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically, once scanned the paper records can be destroyed. It is recommended the paper copies of the record will be retained until independent record integrity assurance is provided. In this context, "independent" refers to other than records managers, e.g. IAOs audit, etc. An annual audit will inform accuracy of the scanning process and more efficient retention periods can be established for destruction of the corresponding paper records (due to storage limitations). Any decision must be agreed by the Senior Information Risk Owner, informed by Records Management, Audit, IAO(s), Data Protection Officer and Caldicott Guardian.

5.10.15 Cloud-Based Records

173 Cloud-based solutions are increasingly being implemented across public authorities. The ICO cloud storage guidance must be followed and a data protection impact assessment must be conducted. Where possible NHS Scotland's data must remain within Scotland's boundaries e.g. where SWAN, N3, NHSmail links are available. The preferred solution must have servers that can be traced to Scotland if NHS Scotland's patient data is stored. Important considerations are:

- best practice records management must be applied, regardless if the cloud offers almost unlimited storage capacity. Records must not be kept longer than required;

- changes of cloud solutions or providers may require the transfer of large amounts of records between digital platforms. A risk assessment must be conducted, and future interoperability must be considered prior to commissioning any solution.

5.10.16 E-Disclosure of Evidence (parties in litigation)

174 Refer to the Ministry of Justices Civil Procedure Rules' Rules and Practice Directions as Rule 31 (UK Law) for rules for disclosure and admissibility of electronic records as evidence.

5.10.17 BYOD (Bring Your Own Device) Records

175 Health and social care organisations are data controllers of any records of BYOD nature created within the course of their business unless clearly identified as "Personal" as part of NHS "reasonable personal use" policies. Failure in tagging these records as "personal" makes of them a corporate asset, and as such are subject to this Code of Practice. Special measure must be taken to transfer and return this type of records to the organisation at the end of the contract (employment, commercial etc.). Storage of confidential or patient identifiable data in an unsecure BYOD is a breach of the organisation's policies and the Data Protection Act 2018 and is potentially reportable to the Information Commissioner's Office.

5.10.18 Websites and Intranet

176 Websites and intranets are digital means to present information in an organised manner (record) therefore they are subject to this Code of Practice. It is important to capture variations (updates) to content published in the website/intranet. Websites/intranets must be subject to change management and the history of the record must be traceable (what was published at a point

in time). Methods to recreate websites/intranets must be considered (e.g. crawls to be stored) including for traceability of dynamic content.

5.11 Duplicate Records

177 NHS Boards must adopt a master record approach, where a primary instance of the record is held.

178 Master records should be kept by the authoritative IAO. Access to the master record or any further copies must be restricted to the approval of the original IAO.

179 Copies should always be marked as such (preferably with the identification of the original IAO) to prevent being used as a master record in error.

5.12 Family Records

180 Some therapy services may create family records to create a holistic view of the family and their needs. These records are typically assigned to a lead individual with pointers to other members of the family records and vice versa (individual's records pointing to the family record held within the lead individual record).

181 The Health and social care record system is, however, based on individual independent records keeping for a number of legal reasons, particular for managing confidentiality and disclosures. Special care is therefore required to avoid unauthorised disclosures. Extensive redaction and special consent may be required.

182 Depending on the purpose of the family record, it is important the most appropriate lead individual is identified, depending on the use to be made of the record, e.g. if it is created to inform intervention to a child rather than a parent, the lead should be the child.

183 The retention period depends on the use of the family record. If it is mainly to inform on a particular patient, e.g. a child (lead individual), the record should be kept following rules for children records, unless other conditions apply (e.g. mental health, child abuse inquiries etc.).

184 If the record is to be used, for example, for interventions to the wider family, the record should be kept in line with the longest retention period applicable.

185 When possible, the record should contain only anonymised data of other members of the family.

5.13 General Practitioner Records

186 GP records are the primary record of care. These records, if in paper, must be preserved for the lifetime of the patient, and at least three years after death (longer periods may apply for specific records, e.g. Child Abuse Inquiries, appraisal for permanent retention rules etc.). If electronic, they must be kept in perpetuity.

187 Discharge letters and further correspondence for other services, including secondary care, must be attached to the main record.

188 The GP record transfers with the individual as they change GP throughout their lifetime.

189 Considerations in section 5.8 are also applicable to GP records when related to provision of functions conferred to the NHS by enactment and subcontracted with private General Practices (data processors, subcontractors and changes in contracts).

190 Scottish Clinical Information in Practice (SCIMP) have produced the 'Good Practice Guidelines for General Practice Electronic Patient Records' for Scottish guidance on the transfer of electronic health records. GPs have an obligation to have regard to any guidelines concerning good practice in the keeping of electronic patient records.

191 SCIMP have produced a simple guide to Scanning and Document Management in General Practice, which covers the implementation of the single scanning and document management system that has now been procured for Scottish General Practices.

192 Where the patient does not come back to the practice and the records are not transferred to a new provider, the record must be retained for 100 years if in paper or permanently if it is electronic.

193 If the patient comes back within 100 years, the retention reverts to 3 years after death (paper records) or permanently if is an electronic record.

5.14 Human Fertilisation

194 The Human Fertilisation and Embryology Authority Code of Practice refers to specific retention period as per Direction 0012[10] .

[10]Human Fertilisation and Embryology Authority – Code of Practice 8.0 (2017 review) www.hfea.gov.uk

195 Licensed centres must retain a record with information about the patient or donor for traceability purposes for a period of at least 30 years from the date on which any gametes or embryos were used in treatment or, if not so used, the date on which any gametes or embryos were removed from storage.

196 In circumstances where the centre is unable to confirm whether or not that patient has given birth to a child as a result of the treatment undertaken at that centre, the record must be kept for 50 years.

197 Additional information related to the safety and quality of gametes and embryos must be kept for a period of at least 10 years after the use of gametes or embryos in treatment.

198 Research projects in this area must keep some minimum details for three years from the date the final report of any research project is submitted to the authority (e.g. number of embryos created, used or dispose, results, conclusions etc.)

199 Refer to the full Direction 0012 (2015) for further details http://ifqtesting.blob.core.windows.net/umbraco-website/1558/2017-04-03-general-direction-0012-version-3-final.pdf. Also available from the Human Fertilisation and Embryology Authority (HFEA) website https://www.hfea.gov.uk/media/2793/2019-01-03-code-of-practice-9th-edition-v2.pdf

5.15 Integrated Records

200 Integrated or joint care records held within Health and Social Care Partnerships are subject to local information sharing agreements. The partnership must agree on ownership, liabilities, security measures, access etc. The partnership must acknowledge the legal basis for the processing across the partnership and the individual organisations purposes.

201 There is not prescribed approached and options included, but are not limited to the following:

- the use of portals and other transient records, where the source of a portion of the integrated record remains owner of the record (data controller) and the other party only has access to share the relevant information;
- to keep a pool of integrated records with joint responsibilities;

Regardless the approach taken for integrating health and care records, an information sharing agreement should be in place and records management rules must be mutually agreed. The NHSS Information Sharing Toolkit must be used wherever NHSS data is concerned.

202 Specific work instructions must be documented to support the operational rules for managing those records by the integrated teams and/or the corresponding records managers.

5.16 Long Term Conditions (LTC)

203 These records are necessary for continuity of clinical care. The primary record of the illness and course of treatment must be kept of a patient where the illness may reoccur or is a life long illness. The primary/master health record is the GP record.

204 This approach is consistent with the direction of NHSS moving towards a more shared service model, where the GP record holds the lifetime view of the patient health. Many patients with long term conditions may have an episode of care in secondary care; the corresponding discharge letters should be kept within the GP record.

5.17 Mental Health Records

205 Mental Health records are where the person has been cared for under the Mental Health (Care and Treatment) (Scotland) Act 2003 as amended by the Mental Health (Scotland) Act 2015. This includes psychology records.

206 Records for any person who has been sectioned under the Mental Health (Care and Treatment) (Scotland) Act 2003, and where care is ongoing the record should be kept until the care is complete and 20 years after last contact. The records of patients with mild forms of adult mental health and are treated in a community setting and where a full recovery is made should be kept for eight years after discharge. All records must be reviewed prior to their destruction taking into account any serious incidents.

207 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 for the additional 10-year period.

208 Mental health entries added into other records must reference the master mental health record and this must not alter the original retention period of the "other" record (where the referenced entry has been done).

209 When the records reach 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.

210 In circumstances when records are released to external bodies for review only, the relevant data should be provided, depending on the purpose for which the record is shared. The justification of the need must be documented, and a note of the sharing added to the record. The justification and details of the type of data shared and recipients should be notified to the Data Protection Officer or the person responsible for the Information Asset Register.

5.18 Occupational Health Records

211 Occupational health records must be kept separate from the main staff record and classified as a health record (whereas the staff record is classified as a corporate record).

212 A summary or report could be kept along with the main staff record only if agreed by the employee.

213 When occupational health records are outsourced, the data controller must ensure the data processor/contractor can retain the records for the necessary period after the termination of service in order for the records to be returned back to the health board.

5.19 Oncology Records

214 Oncology records refer to the master oncology record held by oncology teams with regards to surgical or non-surgical treatment, diagnosis, plan construction information, radiation dose, three-dimensional dose distribution information, imaging, systemic anticancer therapy delivered etc.

215 This Code of Practice also applies to the regional oncology centre record (i.e. radiotherapy and chemotherapy).

216 The Royal College of Radiologists[11] continues to advocate the view that premature destruction of relevant oncology records may result in preventable death, inappropriate subsequent treatment or inadequate response to a patient's lifetime enquiries. For the purposes of clinical care diagnosis, records of any cancer must be retained in case of future reoccurrence. Where the oncology records are in a main health record, the entire file must be retained.

217 Wherever possible, oncology records should be in a preserved electronic format.

218 Oncology records should be reviewed and considered for permanent preservation. The review should be undertaken by the patient's treating clinician or, in their absence, the clinical head of radiotherapy services.

[11] https://www.rcr.ac.uk/sites/default/files/statement_retention_oncology_records_may2017.pdf

219 Any oncology record must be reviewed prior to deletion taking into account any potential long-term research value which may require consent or anonymisation of the record.

5.20 Patient/Client Held Records

220 This Code of Practice does not refer to personally-held records that the subject of care keeps and controls, but records that are left with the individual for different reasons, e.g. to allow care at home by different health and social care teams, some maternity files.

221 In these cases, the record held by the patient/client must have a clear identification that it is a patient-held record and that they remain the property of the data controller and include a return address if they are lost.

222 If these records are the only source of evidence of the treatment or care, they must be transferred to the main health or care record at the end of the treatment that originated the need for the record to be held by the patient/client.

223 For records permanently retained by the patient/client, the health and/or social care organisation must ensure the data is accurate. The information must be replicated into the health and/or social care files.

5.21 Prison, Youth Offenders & Secure Units (Mental) Health records

224 All healthcare records for prisoners should be kept within the GP record. When a GP is assigned to a prison service, a summary of the GP master record must be transferred to the designated prison GP. Where the sentence is for less than six months, episodic records should be treated as hospital episodes and a summary transferred to the main GP record at the end of the sentence with a discharge letter. The original episodic record is subject to the six years adult rule retention unless other conditions apply (e.g. mental health, appraisal of record etc.). Where the sentence is for more than six months, the record should be treated as a normal GP record and transferred to the main GP record along with a discharge letter (could be the original or a new GP if the prisoner has moved or been relocated). Where a patient is sent to prison the original GP record must not be destroyed until the normal retention periods of GP records have been met.

225 **Youth Offending Service Records.** The health and social care portion of these records are subject to this Code of Practice, e.g. for child health records the retention period generally follows the 25th / 26th birthday unless other criteria apply (e.g. mental health, Child Abuse Inquiries, appraisal for permanent retention etc.).

226 **Secure Units for Patients Detained Under the Mental Health (Treatment and Care) (Scotland) Act 2003.** Some institutions that care for offenders are categorised as hospitals because the offender is considered a patient. Such health records are classed as mental health records and must be retained for longer periods of time and normally in excess of 30 years for purposes of the continuity of care or another lawful basis for continued retention.

5.22 Records Dealt with Under the NHS Trusts and Primary Care Trusts (Sexually Transmitted Disease) Directions 2000

227 These records must be treated as particularly sensitive. Current legislation require that special confidentiality and unauthorised disclosure controls are in place to ensure information about sexually transmitted diseases are treated appropriately. Special restrictions for sharing this type of information apply, for these reasons it is common practice these records are managed separately from the main health record.

5.23 Specimens and Samples

228 The retention of human material is not in scope of this Code of Practice. The metadata or records regarding the sample or specimen are, however, covered by this Code of Practice. Relevant professional bodies such as the Human Tissue Authority or the Royal College of Pathologists have issued guidance on how long to keep human material.

229 As human material is not kept for long periods, this does not mean that the information about the specimen or sample should be destroyed at the same time. The information about any process involving human material must be kept for continuity of care and legal obligations. The correct place to keep information about the patient is within the health record and although pathology reports may be retained by the individual pathology departments, a copy must always be included on the health record.

230 The General Data Protection Regulation defines genetic data as personal data within the special categories, therefore records must be processed according to the special categories' rules.

5.24 Staff Records

231 Staff records should hold sufficient information about a staff member for decisions to be made about employment matters. Staff files held by Human Resources must be the central repository for employee information.

232 A master record for each employee should be held by the corresponding Human Resources department. Once the employee moves to a different post or leaves the organisation any departmental employment file should be

reviewed, summarised and transferred to the Human Resources department master record.

233 Where a summary is made it must contain as a minimum:

- a summary of the employment history with dates;
- pension information including eligibility;
- any work-related injury;
- any exposure to asbestos, radiation and other chemicals which may cause illness in later life;
- professional training history and professional qualifications related to the delivery of care;
- list of buildings where the member of staff worked, and the dates worked in each location.

234 Upon termination of contract, records must be held at least up to their statutory retirement age. To reduce the burden of storage and for reasons of confidentiality, it is recommended that a summary be prepared and held until the employee's 75th birthday or six years after leaving whichever is the longer and then reviewed. The summary must have enough detail (refer to minimum list above).

235 It is recommended that the following is adhered to for staff training records:

- clinical training records to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer;
- statutory and mandatory training records to be kept for ten years after training completed;
- other training records should be kept for six years after training completed.

5.25 Transgender Persons Health Records

236 **Please note that this section of the Code of Practice is currently work in progress.**

237 The Medical and Dental Defence Union of Scotland issued medicolegal guidance that either a Gender Recognition Certificate (GRC) nor a statutory declaration are required for change of name and gender on their GP record.

https://www.mddus.com/resources/resource-library/case-of-the-month/2017/february/transgender-records.[12]

238 The General Medical Council (GMC) UK code of practice on transgender healthcare makes it clear that a GRC is not required, and reiterates that the gender history of a patient cannot be shared or disclosed without consent. The GMC Ethnical Hub provides a collection of resources exploring how to apply GMC guidance in practice, focusing on key areas of concern – https://www.gmc-uk.org/ethical-guidance/ethical-hub/trans-healthcare#confidentiality-equality.

239 The Common Services Agency (commonly known as NHS National Services Scotland (NSS)) also issued information on the requirements for processing a change of gender and title – see https://nhsnss.org/foi-disclosure/requirements-for-processing-a-change-of-gender-and-title/.

5.26 Witness Protection Health Records

240 These records are subject to greater security and confidentiality measures. The right to anonymity extends to medical records. A new CHI number is assigned, and a new set of health records must be created.

241 Relevant data necessary for continuity of care must be recreated in the new record. If transferring data from previous records, special redaction measures must be taken to ensure anonymity is guaranteed.

[12] Please note that some of the content of the linked page is not concerned with records management issues but reference implications for a patient for screening.

5.27 Further Guidance, Websites and Links

Regulatory Bodies:

- National Records of Scotland
- Information Commissioner's Office
- Scottish Information Commissioner's Office

Legislation:

- Public Records (Scotland) Act 2011
- Data Protection Act 2018
- General Data Protection Regulations 2016
- Freedom of Information (Scotland) Act 2002

SECTION 6 - The Management, Retention and Disposal of Personal Health Records

6.1 Scope of Schedule

242 This section sets out the recommended 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 GDPR), either due to their on-going administrative value or as a result of statutory requirement. It also provides guidance on dealing with records which have on-going research or historical value and should be selected for permanent preservation and transferred to an appropriate archive.

243 The section 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, emails, X-rays, photographs, CD-ROMs) in which they are created or held.

244 This section does not provide specific guidelines on determining which documents are retained as part of a personal health record. However, 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 weeding) 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 data protection legislation, which states that only personal information which is relevant and not excessive should be retained.

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

- the retention periods in this schedule must be adopted. However, local business requirements or risk analysis may require some categories of records to be kept for longer;

- the provisions of the UK Data Protection legislation and the Freedom of Information (Scotland) Act 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. This applies to records whose use cannot be anticipated fully at the present time, but which may be of value to future generations;

- some classes of document must be permanently preserved and the advice of the local NHS archivist or National Records of Scotland regarding an appropriate place of deposit should be obtained;

- 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. Local procedures should be drafted, 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;

- records which, having been retained for the 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. Where deletion or destruction is not technically feasible, the record should be made permanently inaccessible to all reasonable measures e.g. deleting encryption keys for that record.

246 Guidance on corporate (i.e. administrative, non-health) records commonly found within NHS organisations is given in Section 7. These rules apply equally to the schedules contained there.

6.2 Responsibilities and Decision Making

247 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.

248 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 Healthcare Improvement Scotland. These include standards applicable to administrative and health records.

6.3 Retention Periods

249 Each organisation should produce its own retention schedule, specifying the locally agreed retention periods, in the light of its own internal requirements and those derived from the integration of Health and Social Care Services.

250 Organisations will need to bear in mind the need to retain records where there is any risk that they may be required to consider/defend any legal actions.

251 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.

252 Organisations should ensure that they are able to justify, particularly in terms of the Data Protection Act 2018 when applicable, the retention of records for longer than the recommended period set out in this schedule.

253 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 three years from the date on which the pursuer was aware of the defect and aware that the damage was caused by the defect. It will be for NHS Boards and GPs to make their own judgement in such cases on whether any health records should be retained for this recommended period in order to defend any action brought under the Consumer Protection Act 1987.

254 Organisations should ensure that they have mechanisms in place to identify records for which the appropriate retention period has expired, in line with the 5th principle of the Data Protection Act 2018. It is acknowledged that organisations 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, 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 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.

6.4 Disposal and Destruction of Personal Health Records

6.4.1 Decision Making

255 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.

256 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.

257 Once the appropriate 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.

6.4.2 Disposal and Destruction

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

- **Review:** records may need to be kept for longer than the retention period due to ongoing administrative and/or clinical need. As part of the review, the organisation should have regard to data protection legislation, 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 recommended, the internal retention schedules will need to be amended accordingly and a further review date set. Otherwise, one of the following will apply;

- **Appraisal and Transfer:** to the boards designated place of deposit or consult an NHS archivist or the National Records of Scotland: if the records have no ongoing administrative value but have, or may have, long-term historical or research value. This is a compulsory element under the terms of the Public Records (Scotland) Act 2011. Organisations that do not have their own archivist should consult an NHS Archivist or the National Records 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 legislation.

6.5 Interpretation of the Schedule

259 The following types of record are covered by this retention schedule (regardless of the media on which they are held, including paper, electronic, still and video images, and sound, and including all records of NHS patients treated on behalf of the NHS in the private health sector or NHS patients' records flowing through integrated Health and Social Care Services):

- 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;
- x-ray and imaging reports, output and images;
- photographs, slides and other images;
- microform (i.e. microfiche/microfilm);
- audio and video recordings;
- interaction records (i.e. screen recordings, web chat, SMS text or messaging application logs);
- emails;
- records held on computer, including local, remote and cloud-bases computing;
- scanned documents.

260 The layout and some of the content of the schedules is based on that published by the Information Governance Alliance on 20 July 2016 in its publication: 'Records management: code of practice for health and social care. Find out more here.

261 The Schedules are organised into a table with three headings:

- **Record Type:** lists alphabetically records created as part of a particular function.

- **Retention Period:** specifies the shortest period 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 period, it can vary the period accordingly and record the decision on its own retention schedule. In this regard, however, organisations must consider data protection legislation, 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.

262 The following **'standard' retention periods** apply to the following record types (Table 1)

Table 1 Standard retention periods.

Health Record Type	Recommended Retention Period
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.
Mentally disordered person (within the meaning of any Mental Health Act)	20 years after date of last contact between the patient and any health/care professional employed by the mental health provider, or 3 years after the death of the patient if sooner and the patient died while in the care of the organisation. 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. 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. When the records come to the end of their retention period, they must be reviewed and not automatically destroyed. Such a review should consider any genetic implications of the patient's illness. If it is decided to retain the records, they should be subject to regular review.
Records where the age and type of record cannot be determined	Where a record can no longer be read due to technology being redundant, or because the record does not contain accurate age information, or if it is considered for those records, such as tapes where the records are mixed, and cannot be selectively destroyed. Such records should be retained 25 years since it is possible/probable that they will contain a patient who was one year at the time of interaction.

6.6 Health Records Retention Schedule

Records must follow these retention periods regardless of their format (e.g. paper or electronic). NHS organisations must ensure new systems have functionality in place to allow automation of retention periods and take reasonable plans to resolve legacy system restrictions on this regard.

6.6.1 Core Recommended Retention Periods

Record Type	Recommended retention period	Notes
Adult Health Record	6 years after the date of last entry or 3 years after date of death if earlier (Scottish Prescriptions & Limitations Act.) Refer to GP Records when applicable.	Refer to GP records for notes on prisoners' records being transferred to GP files.
Adult Integrated Health and Social Care Records	Longest retention period amongst regulations applicable to the partnership (e.g. IJBs) or the individual partners.	In cases where a record is held jointly by health professionals and by social care professionals the record should be retained for the longest period for that type of record, i.e. if social care has a longer retention period than health, then the record should be kept for the longer period. The SCARRS 2 Retention Schedule includes a range of timescales for different types of Adult Social Care Records. There is no single retention period for all the record types. http://www.scottisharchives.org.uk/scarrs/schedules. e.g. Integrated Mental Health Case Records – where service user was sectioned under the Mental Health Act. Retain 20 Years from date of last contact or 3 years after death.
Children's Health Records	Retain until the patient's 25th birthday or 26th if young person	It is recommended retaining deceased children patient records for the same period as live patients. Paediatricians have requested that these are retained,

Record Type	Recommended retention period	Notes
	was 17 at conclusion of treatment or 3 years after death.	both considering the Child Abuse Inquiry and to enable the availability of records to assist in the treatment of siblings. The definition of a Children's records does not include CAHMS as these fall within Mental Health.
GP Patient records **MASTER PATIENT RECORD** (including armed forces and prisoners)	Retain for the lifetime of the patient and for 3 years after their death.	Where the patient does not come back to the practice and the records are not transferred to a new provider, the record must be retained for 100 years. If the patient comes back within 100 years, the retention reverts to 3 years after death. Electronic records must be kept in perpetuity.
Records where the age of the patient within the records cannot be determined	Retain for 25 years from date of recording.	Where there is a lack of information in the record, or the technology is no longer available to read the record.

6.6.2 Specialty Records Retention Periods

Record Type	Recommended retention period	Notes
A&E Records	Retain according to core/specialty record e.g. adult/child health record	

A&E Register	8 years after the year to which they relate	
Abortion Certificates	3 years beginning with the date of termination	
Ambulance records – patient identifiable component	7 years	
Audiology records	Retain according to core record rules e.g. adult/child health record	
Breast screening x-rays	9 years from last attendance and 9 years from date of death	The Scottish Breast Screening Programme the x-rays are retained for 9 years from the last attendance and 9 years from date of death.
NHS 24 Webchat	Breathing Space 7 days all others one month.	Does not include those with police involvement, which have a retention of 6 months.
Cervical screening slides	10 years	
Child and Family guidance	Retain according to core record rules e.g. adult/child health record	
Child Protection Register	Retain according to core record rules e.g. adult/child health record	
Clinical psychology	30 years	

Contraception, sexual health, family planning and GU Medicine	adult/child health record rules if implant/device inserted 10y Family Planning: 10 years or 25th/26th birthday rule	GUM: Retain according to adult/child health record rules unless is an implant or device inserted, in which case is 10 years. Family Planning: 10 years after the closure of the case (25th/26th birthday rule for children).
Creutzfeldt–Jakob disease (CJD) records	Permanent	After the retention period should be subject to appraisal for archival preservation until a cure is identified
Dental epidemiological surveys	30 years	
Dietetic and nutrition	Retain according to core record rules e.g. adult/child health record	
General Dental Services Records (Dental and auditory screening records)	Adults: 10 years Children: 10 years or up to 25th/26th birthday rule, whichever is longer.	
Human Fertilisation	3, 10, 30 or 50 years	Refer to section 5.14 Human Fertilisation Records. Refer to Human Fertilisation and Embryology Authority (HFEA) guidance - General Direction 0012 Retention of Records
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.	
Mental Health Records	20 years after date of last contact, or 3 years after death (except with integrated care records)	This refers to discrete mental health record types, when the patient was admitted to an acute hospital for something else that must be part of the appropriate specialty record. In the case of deaths post patients being discharged from Mental Health services, the record still must be retained based on the criteria in this schedule. Cases under Significant Adverse Event Review or with potential genetic associations should be sent for appraisal for permanent retention (recommended). (refer to useful guidance for mental health records in section 5.16)
Mentally disordered persons (within the meaning of any Mental Health Act)	Retain according to core/specialty record e.g. adult/child health record	
Midwifery records	25 years after the birth of the last child	
Neonatal screening records	25 years	
Obstetric records, maternity records and antenatal and postnatal records	25 years after the birth of the last child or until woman reaches age 50, whichever is longer.	Greater occurrence of women giving birth at more spaced periods of time until later in life.
Occupational therapy records	Retain according to core/specialty record e.g. adult/child health record	

Oncology	30 years or 3 years after death	Oncology entries in other records should not alter the original retention period of the record, considering the regional record is kept for 30 years. (refer to “Useful guidelines for Oncology records in section 5.19)
Ophthalmic records	Adults: 7 years Children: 7 years or up to 25th birthday, whichever is longer	
Orthoptic records	Retain according to core/specialty record e.g. adult/child health record	
Physiotherapy records	Retain according to core/specialty record e.g. adult/child health record	
Podiatry	Retain according to core/specialty record e.g. adult/child health record	
Speech and language therapy records	Retain according to core/specialty record e.g. adult/child health record	
Unscheduled primary care records (patient identifiable component)	7 years	Including NHS 24 unscheduled care records, and primary care out of hours services.
Learning difficulties	Retain according to core record rules e.g. adult/child health record	

NHS 24 schedule care services	7 years	
NHS 24 Web Chat Interaction	Retain according to locally specified service specific retention period.	Retention periods for the web chat interaction record will vary depending on the specific service. The individual retention period for each service will be specified in the Board specific Retention Schedule.

6.6.3 Pathology (sub-categories)

Record Type	Recommended retention period	Notes
Screening, including cervical screening, information where no cancer/illness detected is detected	10 years from creation	
Mortuary Records of deceased	10 years	
Mortuary Register	Permanent	Recommend to retain permanently and suitable for archive after 2 years.
Post Mortem Records	30 years	
Disposal of Foetal Tissue Records	8 years after the last entry	

Forensic medicine records	30 years	
Human tissue (within the meaning of the Human Tissue (Scotland Act 2006) – see Forensic Medicine	For post mortem records which from 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.	

6.6.4 Births, Deaths & Adoption Records

Record Type	Recommended retention period	Notes
Birth Notification to Child Health	25 years from receipt by Child Health Department.	Treat as a part of the child's health record if not already stored within health record such as the health visiting record.
Birth Registers	2 years	Where registers of all the births that have taken place in a particular hospital/birth centre exist, these will have archival value and should be retained for 25 years and transferred to a place of deposit (archives) at the end of this retention period.
Body Release Forms	2 years	
Death – cause of death certificate counterfoil	2 years	NHS Scotland is moving to all death certification via eMCCD.

Local Authority Adoption Record	(normally held by the local authority children's services)	Refer to SCARRS: Scottish Council on Archives Records Retention Schedules
NHS Medicals for Adoption Records	Retain as for child/adult records.	

6.6.5 Clinical Trials & Research

For clinical trials record retention please see the MHRA https://www.tsoshop.co.uk/Medical/MHRA/Good-Clinical-Practice-Guide/?TrackID-000039

Record Type	Recommended retention period	Notes
Advanced Medical Therapy Research Master File	30 years after expiry date of the product or longer if required by the Clinical Trial Authorisation	See guidance Good Clinical Practice Guide "Grey Book" Review and consider transfer to a Place of Deposit
Clinical Trials Master File of a trial authorised under the European portal under Regulation (EU) No 536/2014	archive content of TMF or at least 25 years after the end of the clinical trial.	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.158.01.0001.01.ENG Review and consider transfer to a Place of Deposit The Clinical Trials Master File is not held by Research and Development – in general this is held by the Sponsor.

European Commission Authorisation (certificate or letter) to enable marketing and sale within the EU member states area	15 years from closure of trial	http://ec.europa.eu/health/files/eudralex/vol-2/a/vol2a_chap1_2013-06_en.pdf Review and consider transfer to a Place of Deposit
Research data sets	As approved by PBPP (Public Benefit and Privacy Panel) on research application	https:///www.jisc.ac.uk/guides/records-retention-management Review and consider transfer to a Place of Deposit
Research Ethics Committee's documentation for research proposal	5 years from end of research Review and consider transfer to a Place of Deposit	For details please see: http://www.hra.nhs.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/ Data must be held for sufficient time to allow any questions about the research to be answered. Depending on the type of research the data may not need to be kept once the purpose has expired. For example, data used for passing an academic exam may be destroyed once the exam has been passed and there is no further academic need to hold the data. For more significant research a place of deposit may be interested in holding the research. It is best practice to consider this at the outset of research and orphaned personal data can inadvertently cause a data breach.
Research Ethics Committee's minutes and papers	Before 20 years from year to which they relate Review and consider transfer to a Place of Deposit	Committee papers must be transferred to a place of deposit as a public record: http://www.hra.nhs.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/

6.6.6 Cross-specialty records

Record Type	Recommended retention period	Notes
Admission books (paper)	8 years after the last entry	
Allied Health Professionals (AHP) Records	Retain according to core/specialty record e.g. adult/child health record	
Blood bank register	30 years	
Chaplaincy records	2 years	
Clinical Audit	5 years	
Clinical Diaries	2 years	It is not good practice record patient identifiable information in diaries. Patient relevant information should be transferred to the patient record.
Clinical Protocols	25 years	

Record Type	Recommended retention period	Notes
Counselling records	30 years	
Destruction Certificates in relation to health records	Permanently Electronic – archival preservation in Archives.	Records of destruction of individual health records and other health records contained in this retention schedule, including Electronic records, Metadata, destruction stubs, records of clinical information held on destroyed physical media.
Discharge books (paper)	8 years after the last entry	
District nursing records	Retain according to core/specialty record e.g. adult/child health record	
Donor records	30 years post transplantation	
Genetic Records	30 years from date of last attendance	
GP temporary resident forms	Add to primary GP record (registered GP).	Copies in circulation (e.g. with PSD) to be destroyed when scanned or when registered GP confirms reception.
Health Records for classified persons under medical surveillance	50 years from the date of last entry or age 75, whichever is the longer	
Health Visitor records	10 years. Children until 25th birthday	

Record Type	Recommended retention period	Notes
Homicide/Serious Untoward Incident records		Consider transfer for archival preservation
Hospital acquired infection records	6 years	
Intensive Care Unit Charts	Retain according to core/specialty record e.g. adult/child health record	
Macmillan patient records – community and acute	Retain according to core/specialty record e.g. adult/child health record	
Medical illustrations	Retain according to core/specialty record e.g. adult/child health record	
Microfilm/microfiche records relating to patient care	Retain according to core/specialty record e.g. adult/child health record	
Music therapy records	Retain according to core/specialty record e.g. adult/child health record	
Notifiable disease book	6 years	Consider for appraisal for archival preservation.

Record Type	Recommended retention period	Notes
Operating theatre records	8 years after the year which they relate.	Consult with the organisation's designated archive about potential transfer for archival preservation.
Out-patient lists (paper)	2 years after the year to which they relate	
Patient held records	Refer to patient held records schedules	
Personal exposure of an identifiable employee monitoring record	40 years from exposure date	
Photographs	Retain according to core/specialty record e.g. adult/child health record	
Private patient records admitted under section 57 of the National Health Service (Scotland) Act 1978 etc	Retain according to core/specialty record e.g. adult/child health record	
Record of long-term illness or an illness that may reoccur	Lifetime and 6 years after death	Refer to further guidelines in section 5.16 Long Term Conditions (LTC)
Recorded conversation which may be later needed	3 years from creation	

Record Type	Recommended retention period	Notes
for clinical negligence purpose		
Referrals not accepted	Same as speciality/patient type of record (e.g. adult health)	
Scanned records relating to patient care	Retain according to core/specialty record e.g. adult/child health record	
School health records	Retain according to core/specialty record e.g. adult/child health record	
Smoking cessation	6 years from closure of 12 week quit period.	
Telemedicine records (clinician to patient)	Retain according to core/specialty record e.g. adult/child health record	
Transplantation records	Lifetime or 3 years after death. Transfer for permanent archival.	See guidance at https://www.hta.gov.uk/codes-practice Records that relate to investigations or storage of specimens relevant to organ transplantation should be kept for 3 years.
Ultrasound records	Retain according to core/specialty record e.g. adult/child health record	

Record Type	Recommended retention period	Notes
Video records/voice/screen recordings (clinician to patient)	Same retention as main record (child/adult/specialty) Or 7 years (triage output transferred to patient record)	Where the primary purpose of the voice recording is for patient triage and the output is recorded within the patients GP record (which is then retained according to the standard minimum retention period for the patient/specialty at pages 46-47) the audio recording need only be retained for 7 years
Ward registers	2 years after the year to which they relate	
X-ray films	Refer to medical illustrations	
X-ray registers (paper)	30 years	
X-ray reports	Retain according to core/specialty record e.g. adult/child health record	

SECTION 7 - The Management, Retention and Disposal of Administrative Records

This schedule sets out recommended periods for which the various administrative records created within the NHS or predecessor bodies should be retained (in line with data protection legislation), 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.

Appraisal of records after the recommended period should determine whether records are sent for archival preservation, destroyed or retained for a further period (for research, business or legal reasons).

Refer to section 4.7 for further guidance on retention and disposal arrangements.

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

- The retention periods in this schedule must be adopted. However, local business requirements or risk analysis may require some categories of records to be kept for longer.

- Recommended retention periods should be calculated from the suggested trigger point

- The provisions of the Freedom of Information (Scotland) Act 2002 and data protection legislation 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 this applies to records whose use cannot be anticipated fully at the present time, but which may be of value to future generations.

Some classes of document must be permanently preserved and the advice of the local NHS archivist, National Records of Scotland or the Scottish Government eHealth Directorate regarding an appropriate place of deposit should be obtained. This is a compulsory element under the terms of the Public Records (Scotland) Act 2011 Section 1 2(b)(iii)

- 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.

- Files and documents which, having been retained for the 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

Communications

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
1	**Communications**			
1.1	**Communication Services**			
1.1.1	Campaigns (including marketing) – final outputs	Conclusion of campaign	3 years	Relates to campaign workings i.e. adverts/documents/artwork. Consider transfer to archive
1.1.2	Corporate Identity and Branding – artwork	Superseded	Permanent	Consider transfer to archive
1.1.3	Diaries – non-clinical (paper and electronic)	End of diary year	2 years	
1.1.4	Language translation services	End of current year	3 years	
1.1.5	Photographs – corporate and publicity	Date of photograph	10 years	Photographs which would be considered of historical significance should be kept. Consider for transfer to archive
1.1.6	Publications – major publications (guides, books and other publications)	Date published	Permanent	Retain one set of records only – copies to be destroyed once business use concluded. Consider for transfer to archive
1.2	**Conference**			
1.2.1	Conferences – proceedings, routine paperwork, attendance and presentations	End of Conference	Destroy after conference if no longer required	The authority may wish to keep the correspondence longer for its own business purposes Significant national conference papers should be considered transfer to archive

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
1	**Communications**			
1.3	**Consultations**			
1.3.1	Consultations – responses to external consultations	End of consultation	3 years	
1.4	**Customer Engagement**			
1.4.1	Customer Engagement data (including statistics, trends, staff surveys and customer satisfaction data)	Completion of survey	5 years	
1.5	**Media**			
1.5.1	Media relations records – final outputs	End of financial year	5 years	Consider for transfer to archive
1.5.2	Press cuttings	Date of publication	5 years	Press cuttings which would be considered of significance would be considered for transfer to archive. If utilise a commercial electronic cuttings service, this record type will not need to be retained.
1.5.3	Press release and important internal communications	Release date	6 years	Press releases may form a significant part of the public record of an organisation which may need to be retained. Consider for transfer to archive
1.6	**Web Services**			
1.6.1	Board Website/s	Date of creation	6 years	Consider for web-archiving (for example the web-archiving service provided by NRS)

Corporate Governance

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
2	**Corporate Governance**			
2.1	**Adverse Events**			
2.1.1	Incidents (not serious – adverse events (category II and III)	Closure of investigation	10 years	Review and if no longer needed destroy See 3.3.3 for incidents concerning Control of Substances Hazardous to Health Regulation (COSHH)
2.1.2	Incidents (serious – adverse events (category I)) (SAERS)	Closure of investigation	Permanent	Consider for transfer to archive
2.2	**Board and Formal Decision Making**			
2.2.1	Board and Sub-Committees Meetings – minutes and papers	Date of creation	Permanent	Main committees and sub-committees of NHS Boards and special Health Boards and other meetings of significance for legal, administrative or historical reasons. Consider for transfer to archive
2.2.2	Board Meetings (closed sessions)	Date of creation	Permanent	Consider for transfer to archive
2.2.3	Chief Executive Records	Date of creation	May retain for 20 years	Emails and correspondence should be retained and transferred to an appropriate archival facility if they are considered of archival interest
	Board Members register of interests	Register entry date	6 years	
2.2.4	Committees / Groups / Sub-Committees / Department Meetings not listed in the scheme of delegation to the Board	Date of creation	6 years	Includes minor meetings/projects and departmental business meetings
2.2.5	History of Boards or their predecessor organisations	Date of creation	Permanent	Consider for transfer to archive

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
2	**Corporate Governance**			
2.2.6	History of hospitals	Date of creation	Permanent	Consider for transfer to archive
2.2.7	Hospital service files	Date of creation	Permanent	Consider for transfer to archive
2.2.8	Register of Seals	Date of creation	Permanent	Consider for transfer to archive
2.3	**Complaints**			
2.3.1	Complaint case file without litigation – adults	Closure of complaint	7 years	The complaint is not closed until all subsequent process have ceased. The file must not be kept on the patient file. A separate file must always be maintained.
2.3.2	Complaint case file without litigation – children and young adults	Closure of complaint	Until child is 19 or 7 years after closure of complaint	The complaint is not closed until all subsequent process have ceased. The file must not be kept on the patient file. A separate file must always be maintained.
2.4	**Copyright / Intellectual Property**			
2.4.1	Patent / trademarks / copyright / intellectual property	End of lifetime or patent or termination of licence/action	Lifetime of patent or 6 years from end of licence/action	
2.5	**Corporate Policy**			
2.5.1	Policies, strategies and operating procedures including business plans	Superseded	Permanent	Consider for transfer to archive
2.5.2	Admission, transfer and treatment of patients – policy files	Superseded	Permanent	Consider for transfer to archive
2.6	**Information Governance**			
2.6.1	Freedom of Information (FOI) / Environmental Information Regulations (EIR) requests and responses case files	End of calendar financial year	3 years	Where redactions have been made it is important to keep a copy of the redacted disclosed documents or if that is not practical to keep a summary of the redactions

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
2	**Corporate Governance**			
2.6.2	FOI / EIR requests where there has been a subsequent appeal	Closure of appeal	6 years	
2.6.3	FOI Publication Schemes	Superseded	5 years	
2.6.4	Data Breach Investigation Case Files	Closure of investigation	5 years	If the files are part of an adverse event record, they should be kept for 10 years.
2.6.5	Data Protection Privacy Notices	Superseded	5 years	
2.6.6	Data Protection Impact Assessments	End of lifetime of the system, process or procedure	5 years	
2.6.7	Data Sharing Agreements	Date sharing ceases	5 years	
2.6.8	Data Processing Agreement	End of contract	5 years	
2.6.9	Records Management – destruction register / records of disposal certificates	Date of destruction	Permanent	UK National Archives guidance on Information Management Records. Consider for transfer to archive
2.6.10	Records Management Plan – plan and supporting evidence	Superseded	5 years	
2.6.11	Retention schedules	Superseded	Permanent	UK National Archives guidance on Information Management Records. Consider for transfer to archive.
2.6.12	Data Subject Access Request (DSAR) and disclosure correspondence	Closure of SAR	3 years	
2.6.13	Subject Access Request where there has been a subsequent appeal	Closure of appeal	6 years	
2.7	**Legal Support**			
2.7.1	Litigation file/record (adult)	Date case settled or dropped	7 years	

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
2	**Corporate Governance**			
2.7.2	Litigation file/record (child)	Date case settled or dropped	Until child is 19 or 7 years after case settled or dropped, whichever is later	The Prescription and Limitation (Scotland) Act 1973 s17(3) and Aged of Legal Capacity (Scotland) Act 1991 s1 provide that in the case of injury suffered by a child time does not begin to run until she/he attains legal capacity which is 16. 16 years + 3 years limitation
2.7.3	Board arrangements legally administered by NHS organisations – documents describing terms of foundation / establishment and winding-up	Date of creation	Permanent	Consider for transfer to archive
2.7.4	Board arrangements legally administered by NHS organisations – other documents	End of financial year	6 years	
2.8	**Quality and Performance**			
2.8.1	Non-Clinical quality assurance records, including 'quality improvement tools/records'	End of year to which the assurance relates	12 years	
2.9	**Research and Development**			
2.9.1	Research and development findings by Board Staff (scientific, technological and medical)	Date of creation	Consider findings and reports for archival 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. Consider for transfer to archive
2.10	**Risk Management and Insurance**			
2.10.1	Business continuity planning	Date superseded	5 years	
2.10.2	Certificate of Insurance – employers liability insurance (CNORIS)	Date all obligations and entitlements concluded	Permanent	Prescription and Limitations (Scotland) Act 1973 and 1984. Consider for transfer to archive

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
2	**Corporate Governance**			
2.10.3	Insurance policy documentation / certificates of insurance	Date all obligations and entitlements concluded	Permanent	Prescription and Limitations (Scotland) Act 1973 and 1984. Consider for transfer to archive
2.10.4	Risk Register – the assessment of risks	Date superseded	5 years	Consider for transfer to archive
2.11	**Strategic Planning**			
2.11.1	Corporate Plan / Strategic Service Plan	Superseded	Permanent	Consider for transfer to archive
2.12	**Service Planning**			
2.12.1	Activity monitoring reports	Date agreement ended	6 years	
2.12.2	Area health plans	Date superseded	Permanent	Consider for transfer to archive
2.12.3	Databases - demographic and epidemiological based on data supplied by NHS National Services Scotland	Date superseded	20 years	In accordance with general policies of NHS National Services Scotland Information Services, and any specific terms and conditions imposed by them in relation to particular data sets
2.12.4	Databases – demographic and epidemiological based on survey data	End of survey	20 years	May be retained indefinitely if data quality and potential for future reuse justifies cost of migration / regeneration to new formats and platforms
2.12.5	Nursing homes pre 1 April 2002: registration documents and building plans	Date of creation	Permanent	The regulation of care services was taken over by the Care Commission on 1 April 2002. Consider for transfer to archive
2.12.6	Patient activity data	Date superseded	3 years	
2.12.7	Service development reports	End of financial year	6 years	
2.12.8	Summary bed statistics	Date of creation	Permanent	Consider for transfer to archive

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
2	**Corporate Governance**			
2.12.9	Waiting list monitoring reports	Date superseded	6 years	
2.12.10	Winter business plans	Date superseded	6 years	

Estates and Facilities

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
3	**Estates and Facilities**			
3.1	**Asbestos**			
3.1.1	Asbestos register, equipment monitoring/testing and records of maintenance	Completion of monitoring or test	40 years	Control of Asbestos at Work Regulations 2012
3.2	**Maintenance & Equipment – Non-clinical and Clinical**			
3.2.1	Cleaning schedules	End of lifetime of installation	Lifetime of installation	
3.2.2	Equipment monitoring/testing and maintenance work e.g. boiler, lifts etc	End of lifetime of installation	Lifetime of installation	Should be retained permanently if there is any measurable risk of a liability. Consider for transfer to archive
3.2.3	Inventories (non-current) of items having an operational lifetime of less than 5 years	End of financial year	2 years	
3.2.4	Maintenance request books and logs (includes digital systems and databases)	End of financial year	2 years after financial year referred to	
3.2.5	Manuals – operating, policies and procedures	End of lifetime of equipment	Lifetime of equipment/machinery the manual refers to	
3.2.7	Medical Equipment – decontamination records	Date of decontamination	25 years	
3.3	**Health and Safety**			
3.3.1	Accidents and incident reporting – reporting accidents to adults	Date of entry / Accident book – date of last entry	10 years	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 Prescription and Limitation (Scotland) Act 1973

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
3	**Estates and Facilities**			
3.3.2	Accidents and incident reporting – reporting accidents to children	Date of birth of child	25 years	
3.3.3	Audit forms, Control of Substances Hazardous to Health Regulation (COSHH) documentation, safety risk data sheets, risk assessments and control measures etc	Date of last action	40 years	Control of Substances Hazardous to Health Regulations 2002
3.3.4	Reporting of Injuries, Disease and Dangerous Occurrences Regulations 2013 (RIDDOR) including Accident Register	Date of last entry on register	10 years	
3.3.5	National Safety Alert	Date of creation	Permanent	Covers Drug Alerts, Estates & Facilities Alerts, Safety Action Notices etc.
3.4	**Property and Land Management**			
3.4.1	Buildings – papers relating to occupation, plans and records of major building works	Data of creation	Lifetime of the building or disposal of asset plus six years	Building plans and records of work are potentially of historical interest. Consider for transfer to archive
3.4.2	Building Project Files (£250,000 and over)	Date of creation	Permanent	Including abandoned or deferred projects. Consider for transfer to archive
3.4.3	Building Project Files (under £250,000)	Completion / abandonment of project	6 years	
3.4.4	Capital charges data	Date of creation	3 years after completion of previous 5 years valuation term	
3.4.5	CCTV		See ICO Code of Practice	The length of the retention must be determined by the purposes for which the CCTV has been deployed. The recorded

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
3	**Estates and Facilities**			
				images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated
3.4.6	Contaminated Land	Date of creation	Permanent	Consider for transfer to archive
3.4.7	Decommissioning of NHS Buildings – evidential documentation (e.g. clearance checklists and images)	Date of decommissioning of the building or campus	6 years	
3.4.8	Environmental Information (e.g. Environmental reports)	Date of creation	Permanent	Consider for transfer to archive
3.4.9	Green Code	Date of creation	Permanent	Consider for transfer to archive
3.4.10	Property performance	Date of creation	Permanent	Consider for transfer to archive
3.4.11	Property strategy	Date of creation	Permanent	Consider for transfer to archive
3.4.12	Records of custody and transfer of keys	Date of transfer	2 years	
3.4.13	Site Maps	Date of creation	Permanent	Duplicate site maps are not covered by the requirement to be retained permanently e.g. copies held by CLO Consider for transfer to archive
3.4.14	Sustainability records	End of financial year	6 years	
3.5	**Property Transactions**			
3.5.1	Contracts and agreements	After the end of the contract	6 years	Including non-sealed (property) on termination
	Tenders (unsuccessful)	Date contract awarded to successful bidder	6 years	

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
3	**Estates and Facilities**			
3.5.2	Deeds of title	Date of creation	Permanent	Title deeds are retained on a permanent basis while the property is retained by the NHS but on disposal, the relevant title deeds are required to be transferred to the purchaser. Consider for transfer to archive
3.5.3	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, specification, “as built” record drawings and documents on the appointment and conditions of engagement of private buildings and engineering consultants)	Date of creation	Permanent	Inclusive of major projects abandoned or deferred. Consider for transfer to archive
3.5.4	Land leases, purchase and sale – deeds, maps, surveys, registers etc	Date of creation	Permanent	Consider for transfer to archive
3.5.5	Land purchased and sale – negotiations not completed	Date negotiations concluded or abandoned	6 years	
3.5.6	Property acquisition dossiers	Date of creation	Permanent	Consider for transfer to archive
3.5.7	Property contracts	Date contract ended	6 years	
3.5.8	Property disposal dossiers	Date of creation	Permanent	Consider for transfer to archive
3.5.9	Property management system	Date of creation	Permanent	Consider for transfer to archive

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
3	**Estates and Facilities**			
3.5.10	Property purchases and leases	Date of creation	Permanent	Consider for transfer to archive
3.5.11	Property title deeds	Date of creation	Permanent	Consider for transfer to archive
3.5.12	Property – terriers (NHS premises site information)	Date of creation	Permanent	Consider for transfer to archive
3.5.13	Specifications for work tendered	After completion of works	6 years	
3.6	**Waste Management**			
3.6.1	SEPA Registrations, Licences and Consents	Date of receipt	Permanent	Consider for transfer to archive
3.6.2	Waste Consignment Notes – Controlled wastes such as clinical / healthcare and household / domestic	End of financial year	2 years	
3.6.3	Waste Consignment Notes – Special / Hazardous / Radioactive Wastes	End of financial year	3 years	
3.6.4	Duty of Care Inspection Reports	Date of creation	Permanent, or for life of external contract	Consider for transfer to archive

Financial Management

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
4	**Financial Management**			
4.1	**Financial Provisions Management**			
4.1.1	Accounts – final annual master copies	End of financial year	Permanent	Consider for transfer to archive

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
4	**Financial Management**			
4.1.2	Accounts – includes cost, working papers and minor records, advice notes	After completion of statutory audit	3 years	
4.1.3	Audit – (including original documents, management letters, value for money (VFM) reports and system/final accounts memorandum)	After completion of statutory audit	3 years	A longer period may be required for investigate purposes
4.1.2	Budgeting – including budget monitoring reports	End of financial year	3 years	
4.1.2	Financial plans, estimates recovery plans	End of financial year	6 years	
4.1.3	Funding data	End of current financial year	6 years	
4.1.4	Indemnity Forms	End of financial year after the indemnity has lapsed	6 years	
4.1.5	Ledger Balances	End of financial year	6 years	
4.1.6	Mortgage documents – acquisition, transfer and disposal	Date of creation	Permanent	Consider for transfer to archive
4.1.7	Register of gifts and hospitality received by individual members of staff	Register entry date	6 years	
4.1.8	Benefactions – endowments, legacies gifts etc. received by the health board	End of financial year	8 years	Consider for transfer to archive
4.2	**Financial Transactions Management**			
4.2.1	Bank Statements	After completion of statutory audit	3 years	
4.2.2	Cash books and sheets	End of financial year	6 years	
4.2.3	Creditor payments	End of financial year	6 years	

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
4	**Financial Management**			
4.2.4	Debtor's records (cleared and un-cleared)	Date debt discharged	6 years	Prescription and Limitation (Scotland) Act 1973
4.2.5	Demand Notes	Close of financial year	6 years	
4.2.6	Expenses Claims	End of current financial year	6 years	Taxes Management Act 1970 Keeping VAT Records HMRC Reference Notice 700/21 (October 2013)
4.2.7	Income and expenditure sheets and journals	End of financial year	3 years	
4.2.8	Invoices	End of financial year	6 years	e.g. Invoices payables (creditors), invoices receivable (debtors) and capital paid invoices
4.2.9	Non-exchequer funds records	End of financial year	6 years	
4.2.10	Receipts	End of financial year	3 years	Includes cheques bearing printed receipts
4.2.11	Records of purchasing authorisation limits	Superseded	1 year	
4.3	**Fraud Prevention**			
4.3.1	Inquiries involving fraud / other irregularities	Completion of court proceedings / disciplinary process	6 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. Taxes Management Act 1970 Prescription and Limitation (Scotland) Act 1973
4.3.2	Internal Fraud Reports	End of financial year	6 years	
4.3.3	Annual Report to Counter Fraud Services	End of financial year	6 years	
4.4	**Payroll and Pensions**			

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
4	**Financial Management**			
4.4.1	Pay as You Earn (PAYE) records	End of financial year	6 years	
4.4.2	Salary/Wages Records	End of current tax year	10 years	For superannuation purposes authorities, may wish to retain such records until the subject reaches pensionable age
4.4.3	Statutory Maternity Pay Scheme records	End of current tax year	3 years	The Statutory Maternity Pay (General) Regulations S.I 1986/1960 as amended by SI 2005 No.989
4.4.4	Statutory Sick Pay Scheme records	End of current tax year	3 years	Statutory Sick Pay (General) Regulations S.I 1982/894
4.4.5	Superannuation Records	End of financial year	10 years	Includes accounts – registers and forms
4.4.6	Substitute for Return (SFR) returns	End of financial year	6 years	
4.5	**Procurement**			
4.5.1	Approved suppliers list	Superseded	11 years	
4.5.2	Contracts sealed or unsealed	End of contract	7 years	
4.5.4	Contract management files - including: contract award letters and agreements, post-tender negotiations, service level agreements, compliance reports, performance reports, variations to contracts (revisions, extensions)	End of contract	5 years	Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45
4.5.5	Contracts – GP Practices and others to deliver core NHS services	Date of contract	Permanent	Consider for transfer to archive
4.5.6	Indents	End of financial year	2 years	
4.5.7	Medical equipment specifications – major items purchased	Date of purchase	Permanent	Consider for transfer to archive
4.5.8	Products – liability	Lifetime of Product	11 years	
4.5.9	Purchase ordering records (purchase orders, goods received notes)	End of current financial year	6 years	Keeping VAT records HMRC Reference: Notice 700/21 (October 2013)

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
4	**Financial Management**			
4.5.10	Register of contracts	Expiration/conclusion of contract		Procurement Reform (Scotland) Act 2014. Section 35. The statutory requirement is that register entries for contracts cannot be deleted until contract expires or is terminated. The authority may choose to keep the entries for a longer period for historical purposes
4.5.11	Stock control reports	Date of creation	2 years	
4.5.12	Stores – major (ledgers etc)	Date of creation	6 years	
4.5.13	Stores – minor (requisitions, issue notes, transfer vouchers, goods received books etc)	Date of creation	2 years	
4.5.14	Supplies records – minor (invitations to tender and inadmissible tenders, routine papers relating to catering and demands for furniture, equipment, stationery and other supplies)	Date of creation	2 years	
4.5.15	Tender evaluation, negotiation and notification records (successful)	End of contract	5 years	Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45
4.5.16	Tender evaluation, negotiation and notification records (unsuccessful)	Award of tender	5 years	
4.6	**Taxation**			
4.6.1	Pay as you earn (PAYE) records	End of financial years	6 years	
4.6.2	Substitute for Return (SFR) Returns	End of financial year	6 years	
4.6.3	Tax Forms	End of financial year	6 years	
4.6.4	VAT records	End of financial year	6 years	In some instances, a shorter period may be allowed, but agreement must be obtained from HM Revenue and Customs

Human Resources

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
5	**Human Resources**			
5.1	**Administering Employees**			
5.1.1	Disciplinary – First and Final written warning	Date of termination	6 years	Although the sanction is spent after 12 months, the information relating to the written warning requires to be kept. It forms part of the employee's record which is held for the duration of employment and 6 years after.
5.1.2	Disciplinary – Letter of Dismissal	Date of dismissal	10 years	Where action is in prospect or has been commenced, consult with legal representatives and keep in accordance with advice provided
5.1.3	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	Date of termination	6 years	The Employment Act 2002 deals with dispute resolution but does not give time limits for record retention. Where action is in prospect or has been commenced, consult with legal representatives and keep in accordance with advice provided
5.1.4	Duty Roster / timesheets	Close of financial year	6 years	
5.1.5	Staff Records – including: personnel files, letters of application and appointment, confirmation of qualifications, contracts, joining forms, references and related correspondence, termination forms, leave cards/information	Date of termination	6 years	Consider section 5.24, regarding the retention of summary information.

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
5	**Human Resources**			
5.1.6	Staff Training Records	Date of termination	6 years	Consider section 5.24, regarding the retention of summary information.
	Staff Training Records – Nurses	Completion of training	30 years after completion of training	Applies only to Nurse Training carried out in hospital-based nurse training schools. Consider section 5.24, regarding the retention of summary information.
5.1.7	Grievances	Date of termination	6 years	
5.1.8	Referral to Professional Bodies (GMC/NMC/AHPF)	Date of termination	6 years	Consider retaining records for longer if investigation has not yet been concluded by professional body.
5.1.9	Volunteers Records including: personnel files, letters of application and appointment, confirmation of qualifications, contracts, joining forms, references and related correspondence, termination forms	Date of termination	6 years	
5.1.10	Work force placement records	Date of termination	6 years	
5.2	**Employee Engagement**			
5.2.1	Industrial relations (not routine – including tribunal case records)	Closure of investigation	Permanent	Consider for transfer to archive
5.3	**Occupational Health**			
5.3.1	Health promotion – core papers and visual materials relating to major initiatives	End of promotion	10 years	Consider for transfer to archive
5.3.2	Occupational Health Reports	Date of termination	6 years	Consider paragraph 221, that details Occupational Health Records must be kept separate from the main staff record.
5.4	**Recruitment**			
5.4.1	Applications for employment – unsuccessful applicants	Date of recruitment	1 year	
5.4.2	CVs for non-executive directors – successful	End of term of office	5 years	

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
5	**Human Resources**			
5.4.3	CVs for non-executive directors – unsuccessful		2 years	
5.4.4	Disclosure Scotland information	Date on which recruitment or other decisions have been taken.	90 days	90 days after the date on which recruitment or other relevant decisions have been taken. Certification number and disclosure level can be retained as a summary record.
5.4.5	Job advertisements	Date of advert	1 year	For jobs where unusual patterns of progression are advertised, it is recommended the job advert paperwork is kept for the length of the progression period plus 6 years if a complain exists
5.5	**Equality and Diversity**			
5.5.1	Investigations – Case files	Investigation concludes, and actions is spent / Retain current information throughout employment	6 years / Employment term	
5.5.2	Equalities Papers for publication	Superseded	4 years	Equality Act 2010

Information & Communication Technology

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
6	**Information & Communication Technology**			
6.1	**System Development**			
6.1.2	Development and post-implementation changes to an ICT system	Decommissioning of system	5 years	Consider for transfer to archive
6.2	**Security Management**			
6.2.1	Security protocols for an ICT system	Decommissioning of system	5 years	Prescription and Limitation (Scotland) Act, 1973 and 1984
6.2.2	Opening, maintenance and closure of a user account for an ICT system	Closure of user account	1 year	
6.2.3	Routine monitoring of access to, and use of, an ICT system	End of current year	2 years	
6.2.4	Detection and investigation of security breaches of an ICT system, and action taken	Last action on incident	3 years	
6.3	**Systems Operations Management**			
6.3.1	Routine monitoring and testing of an ICT system, and action taken to rectify problems and optimise performance	End of current year	1 year	
6.3.2	Investigation of faults reported by users of an ICT system, and action taken to rectify problems	Close of investigation	3 years	
6.3.3	Management of data in an ICT system, including the operation of routine data backup, archiving and deletion routines	End of current year	1 year	
6.3.4	Maintenance of the software licence(s) for an ICT system	Expiry/Termination of licence	5 years	Prescription and Limitation (Scotland) Act, 1973 and 1984

	Activity/Record Type	Retention Trigger – event that prompts start of retention period	Recommended Retention Period	Citation/Notes
6	**Information & Communication Technology**			
6.3.5	Management of an ICT system – system file (including handover documents, user guides, system support, technical and knowledge base documentation)	Decommissioning of system	5 years	
6.3.6	Register of removal/return of mobile ICT systems hardware and software from/to Board premises	Return of equipment	5 years	
6.3.7	Disposal log of arrangements for the sanitisation and disposal of institutional ICT equipment	Disposal of equipment	5 years	
6.4	**Systems User Training & Support**			
6.4.1	Development of technical and application training and guidance for IT system users	Superseded	1 year	
6.4.2	Logging, investigation and resolution of user requests for technical and application support	Close of call	1 year	

Annex A: Acknowledgments

The Scottish Government and the NHS Scotland are very grateful to the following that provided their time and expertise on the project group, authoring team and reviewing team developing this update:

e-RECORDS ADVISORY GROUP

- Wendy Barber (Falkirk Council)
- Bryan Lawson (Golden Jubilee National Hospital)
- Chris Morrice (NHS Grampian)
- Elaine Henderson (NHS National Services Scotland)
- George Irvine (Scottish Government)
- Grant Forrest (NHS Fife)
- Sanny Gibson (NHS 24)
- Ernest Beattie (NHS National Services Scotland)

APPRAISAL AND PRESERVATION OF RECORDS ADVISORY GROUP

- Alistair Tough (NHS Greater Glasgow & Clyde)
- Louise William (University of Edinburgh)
- Isobel Brown (NHS Greater Glasgow & Clyde)
- Sharon Stott (Golden Jubilee National Hospital)
- Zarya Rathe (TBC)
- Graham Roberts (TBC)
- Hugh Hagan (National Records of Scotland)
- Ruth Honeybone (University of Edinburgh)

CORPORATE RECORDS ADVISORY GROUP

- John Hamilton (NHS Greater Glasgow & Clyde)
- Lynne Smith (Healthcare Improvement Scotland)
- Kerry Lochrie (NHS Greater Glasgow & Clyde)
- Lynda Petrie (NHS Tayside)
- Natali Higgins (NHS Ayrshire & Arran)
- Tracey Gill (NHS Education Scotland)
- David Morgan (NHS Shetland)

HEALTH RECORDS ADVISORY GROUP

- George Ironside (NHS Borders)
- Karen Mowbray (NHS State Hospital)
- Deirdre Coyle (NHS Forth Valley)
- Wendy McKissack (NHS Forth Valley)
- Maureen Masterton (NHS Lothian)
- Roslynne O'connor (Portree Medical Centre)
- Andrew Vickerstaff (NHS Highland)

- Ian Thomson (GP)
- Robert Bryden (NHS Ayrshire & Arran)

INTEGRATED H&SC RECORDS ADVISORY GROUP

- Alex Fitzgerald (East Lothian Council)
- Roberto Riaviz (West Lothian Council)
- Gordon Laird (Glasgow City Council)
- Henry Sullivan (Edinburgh City Council)
- Jean Still (NHS Greater Glasgow & Clyde)
- John McGonigle (NHS Dumfries & Galloway)
- Lesley Gauld (Fife Council)
- Meic Pierce Owen (Perth & Kinross Council)
- Jillian Neilson (NHS Ayrshire and Arran)
- Carol Dunn (West Lothian Council)

MULTIDISCIPLINARY ADVISORS

- Frank Rankin
- Daniel Beaumont
- Elena Beratarbide

Additionally, we are very grateful to the Information Governance Alliance for their participation and review of the draft version, and for facilitating the National Records Management Workshop,

We are very grateful to the following for the time and effort put into responding to the public consultation:

- NHSS Records Management Forum
- NHSS Information Governance Leads Group
- NHSS Caldicott Guardians Forum
- British Medical Association

Annex B: Standard Setting Bodies

- Academy of Medical Royal Colleges (AoMRC) (hosted by the Royal College of Physicians)

  https://www.rcplondon.ac.uk/projects/outputs/generic-medical-record-keeping-standards

- British Medical Association

  http://bma.org.uk/practical-support-at-work/ethics/confidentiality-and-health-records

- General Medical Council

  http://www.gmc-uk.org/guidance/index.asp

- General Pharmaceutical Council

  https://www.pharmacyregulation.org

- Health and Care Professions Council

  http://www.hcpc-uk.org/

- Nursing and Midwifery Council

  https://www.nmc.org.uk/standards/code/

- Royal College of General Practitioners (with the DH and the BMA)

  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/215680/dh_125350.pdf

- Scottish Clinical Information Management in Practice (SCIMP)
  www.scimp.scot.nhs.uk/

- Royal College of Nursing

  http://www.rcn.org.uk/development/health_care_support_workers/professional_issues/record_keeping

- Royal College of Obstetricians & Gynaecologists

  https://www.rcog.org.uk/en/guidelines-research-services/guidelines/

- Royal College of Pathologists

  http://www.rcpath.org/Resources/RCPath/Migrated%20Resources/Documents/G/G031_RetentionAndStorage_Apr15.pdf

- Royal Pharmaceutical Society
- https://rpharms.com/
- Royal College of Physicians

  https://www.rcpe.ac.uk/
- Royal College of Physicians and Surgeons of Glasgow

  https://rcpsg.ac.uk
- Royal College of Surgeons of Edinburgh

  https://www.rcsed.ac.uk

Annex C: Glossary of Records Management Terms

Note: The National Records of Scotland and 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))

Administrative 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

Data Sharing

The sharing of data between two (or more) parties can either take the form of sharing between joint data controllers or between a data sharer and a data processor.

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))

Document

In general, a document (noun) is a record or the capturing of some event or thing so that the information will not be lost. Usually, ad document is written, but a document can also be mead of pictures and sounds.

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

Health records are the most important tool to support patient care and continuity of that care. The health record is a single record with a unique identifier, which is a composite of all data on a given patient held by an organisation. 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.

ISMS Information Security Management System

An information security management system (ISMS) is a framework of policies and procedures for managing an organisation's information risk to minimise exposure, ensure business continuity and maximise the value of information assets by proactively managing the potential impact of information issues.

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 Records of Scotland has guidance on Metadata Standards 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 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 2011. The information contained in those records is subject to Data Protection and Freedom of Information legislation.

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 archival preservation. Such records should be transferred to an archive, either the organisation's own NHS archive or a local authority, university, or other archive with which the organisation has an existing relationship.

Section 19 of the Data Protection Act 2018 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))

Processing

Processing of information, as defined in the Data Protection Act (2018), includes anything done with records containing data, i.e. holding, obtaining, recording, using, disclosure, sharing, disposal, transfer or destruction.

Protective Marking

The Protective Marking System (often referred to as the Government Protective Marking System/Scheme or GPMS) is the Government's administrative system to ensure that access to information and other assets is correctly managed and safeguarded to an agreed and proportionate level throughout their lifecycle, including creation, storage, transmission and destruction.

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 2011

The Act's purpose is to improve records management in named Scottish public authorities, including NHS Boards. It aims to do this by making it compulsory to produce and maintain Records Management Plans, updating the definition of 'public records', setting up the Keeper's role in compliance monitoring and guidance provisions, and updating the law on records of the Scottish courts.

R

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.

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))

Records Management Plan (defined in the Public Records (Scotland) Act 2011

Part 1 of the Public Records (Scotland) Act 2011 imposes duties on certain public authorities such as NHS Boards to produce, implement and review records management plans.

- The Plan must set out the arrangements for the management of records created or held by the NHS Board and records created or held by contractors who carry out any functions on behalf of the Board.
- Each Plan must identify a coherent governance structure, and list the processes and procedures the Board will undertake to ensure effective management, storage and disposal of records
- Each Plan must be submitted to the Keeper of the Records of Scotland for agreement and, once implemented, be kept under internal review
- Boards must have due regard to the model plan and the guidance issued by the Keeper when preparing their own plans.

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, for example in a Subject Access Request where parts of the health record refers to third-party information. The National Archives provides guidance on redaction, available here

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 right to access information held by public authorities, created by the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004, both of which came into force on 1 January 2005. The Act and the Regulations give anyone, anywhere in the world, important rights to access the information held by more than 10,000 public authorities in Scotland.

Scottish NHS Archivists

Three NHS Boards in Scotland employ archivists: Grampian Lothian, and Glasgow. The funding and managerial arrangements for each of these archives differs, but each collect, lists and preserves corporate and health records of and relating to the NHS

organisations and predecessor bodies and institutions in their local area. Under PRSA all Boards without their own archivist should have a designated place of deposit. 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.

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 UK Data Protection Legislation (the General Data Protection Legislation and the Data Protection Act 2018) and liaises with the Scottish Information Commissioner with regards to the interaction between the Data Protection Act Legislation 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.