Code of Practice

Records Management Code of Practice
for Health and Social Care

A guide to the required standards of practice in the management of data, information and records for those who work within or under contract to NHS organisations in Scotland.

Published – August 2024

Digital Health & Care Scotland
NHS SCOTLAND
Scottish Government
Riaghaltas na h-Alba

Document Control Sheet

Title:	Records Management Code of Practice for Health and Social Care
Date Issued:	16 August 2024
Effective From:	30 August 2024
Version Number:	Version 4.0
Document Type:	Code of Practice
Document status:	Final
Author:	Natali Higgins, Programme Lead – Records Management Code of Practice
Owner:	Digital Health & Care Division, Scottish Government
Contact:	DHCIG@gov.scot
Target Audience:	• Records Management Leads, • Information Governance Leads, • Data Protection Officers, • Caldicott Guardians and • Senior Information Risk Owners All with responsibility to ensure this is cascaded as appropriate.
Supersedes	• Scottish Hospital Service Destruction of Hospital Records (SHM 58/60) • Disposal of Records That Have Lost Their Value (ECS (A) 21/1969) • Guidance for The Retention and Destruction of Health Records (MEL (1993) 152) • The Management; Retention and Disposal of Administrative Records (HDL (2006) 28) • Scottish Government Records Management: NHS Code of Practice (Scotland) Version 1.0 2008 (CEL 28 (2008)) • Scottish Government Records Management: NHS Code of Practice (Scotland) Version 2.0 March 2010 (CEL 31 (2010)) • Scottish Government Records Management: NHS Code of Practice (Scotland) Version 2.1 January 2012 • Scottish Government Records Management: Health and Social Care Code of Practice (Scotland) 2020 (Version 3.0)

Distribution list: open access to this document is available via the Digital Health and Care Website https://www.digihealthcare.scot/resources/

Contents

Section 1 - Introduction

1.1 Background

1 This Code of Practice is a framework to support the consistent approach to, and effective management of, data, information and records. It is based on current legal requirements and professional best practice.

2 It is relevant to NHS Boards, and organisations who work with or under contract to them, to support the delivery of health care services across Scotland. This also includes public health functions in Local Authorities and social care where there is joint care provided within the NHS. Any organisation that processes health care data, information and records under the Public Bodies (Joint Working) (Scotland) Act 2014 should use this Code of Practice, including subcontractors processing data, information and records on behalf of NHS Boards and contracted third party providers.

3 The Code of Practice has been developed by the Scottish Government Digital Health and Care Information Assurance Team, in collaboration with representatives of the Scottish health and social care sector, including records managers, archivists, information governance professionals, clinicians, social care and social work representatives from the NHS, Local Authorities, GP practices, Royal Colleges, and Regulatory Authorities. It 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.

1.2 Strategic Context

4 This Code of Practice plays a pivotal role in supporting the implementation of strategies and policies across health and social care in Scotland.

5 The vision of the current Digital Health and Care Strategy 2021 is: ‘To improve the care and wellbeing of people in Scotland by making best use of digital technologies in the design and delivery of services.’ The strategy also supports the aims of the NHS Recovery Plan in its ambition to address the backlog in care and meet ongoing healthcare needs for people across Scotland. It will support reform of the care system, including better integration of health and care services.

6 This refreshed strategy also provided the framework for the development of Scotland’s first Data Strategy for Health and Social Care. The Data Strategy sets out to ensure that health and care data supports the delivery of health and care services and that it does so in a way that empowers citizens and supports innovation and research.

7 Information is at the core of the health and care strategic direction in Scotland. To achieve the ambitions of both strategies it is crucial that there is a national approach to the management of data, information and records, which is a key aim of this Code of Practice.

- This will result in a more consistent approach to data information and records management across health and care, better enabling the implementation of digital systems and enhancing the interoperability across systems, which ultimately will allow for mitigation of some of the information risks.
- This will enable opportunities for citizens to have a more consistent experience with regards to their information across the health and care system, regardless of their location.
- This will support the improved delivery of services, enabling the sharing of information across health and social care, increasing efficiency and supporting better use of the information held to the benefit of citizens in Scotland.

8 Therefore adoption of the standards within this Code of Practice is fundamental to achieving the vision and aims of the strategies.

9 Going forward, it is acknowledged that, in order to best support integrated working and meet the aims of the Digital Health and Care Strategy and Data Strategy, it will likely be beneficial to develop this Code of Practice to reflect and inform policies and practices across health, social work, and social care more broadly. Work in this area is ongoing, in collaboration with Local Government partners, and it is anticipated that this will be incorporated in future versions of this Code of Practice.

1.3 Aims

10 This Code of Practice aims to harmonise the management of data, information, and records across organisations in order to promote consistency of approach and support the 'Once for Scotland' ethos. It aims to achieve this by:

- outlining records management best practice in relation to the creation, use, storage, management and disposal of data, information, and records (including, where appropriate, the archival preservation of vital and historically important records);
- providing guidance on the general legal obligations that apply to data, information and records within the health care sector;
- setting out recommendations for best practice to assist in fulfilling these obligations, e.g. adhering to information governance and cyber security standards;
- setting out recommended periods of retention for data, information and records held by organisations, regardless of the media on which they are held;
- indicating where further guidance on records management may be found;
- explaining the requirement to select, and transfer to a designated place of deposit, those records for archival preservation.

11 It is important that, where possible, organisations use a consistent approach when managing their data, information and records. This not only supports cross-organisation working and information sharing, it also supports the implementation of national strategies which aim to improve the care and wellbeing of people in Scotland by making best use of data, information, records and digital technologies in the design and delivery of services. This Code of Practice plays an important role in setting out how to manage records and information within such technologies to enable communication, support the integration of care, enhance availability of information, and improve working practices.

1.4 Scope

12 This Code of Practice applies to data, information, and records, in any format, or stage of processing in the delivery of health care functions and associated supporting business services. This includes those handled by third parties on behalf of NHS Boards in connection with health care and associated administrative purposes.

13 Formats include, but are not limited to:

- Paper
- Digital
- Email
- Scanned
- Audio/Video recordings
- Photographs/medical imaging
- Microform (microfiche/microfilm)
- Instant messaging/SMS
- Social media posts
- Website content (internet/intranet)

14 The Code of Practice does not cover the retention of human material, in the form of samples or specimens or dental moulds; however, it does cover any data, information or records associated with them. Further guidance can be found at Section 5.32.

15 The records retention schedule detailed at Annex B does not cover social care and social work records and therefore does not apply to Local Authorities or organisations contracted by them in relation to the delivery of social care and social work services. Local authorities base their retention schedules on standards and guidance provided within the Scottish Council on Archives Record Retention Schedules (SCARRS)[1].

16 Local Authorities should however refer to the retention schedule at Annex B when managing any NHS health and/or corporate records held by them.

17 It is recommended that integrated health and social care records should be held for the longest retention period specified in the Code of Practice or the retention schedule belonging to the associated Local Authority. This information should be documented in the relevant integrated records agreement.

1.5 Document Management

18 This version is a renewed baseline version which further expands into the evolving health and social care sector. It provides generic overarching records management guidance as well as record-specific guidance and signposting to additional professional/industry standards, guidance, further information.

19 The document will be updated on an ongoing basis through a change management process and therefore will be subject to regular change. This will ensure that the document is responsive to changes within the health and social care sector with regards to business need and regulatory/legislative requirements.

20 The change management process will involve review and approval by various stakeholders and professionals depending on the assessed level and context of the requested change.

[1] Scottish Council on Archives Record Retention Schedules (SCARRS) (scottisharchives.org.uk)

Section 2 - Context

2.1 Definitions

21 **Data** is defined as raw, unprocessed information which requires to be organised.

22 **Information** is data that has been processed, structured, and given meaning.

23 **Records** are specific recognised types of collated and organised information and data created, received, and maintained as evidence by an organisation for reference in the transaction of business or pursuance of legal obligations. This definition extends to the archive role, particularly in recording corporate memory.

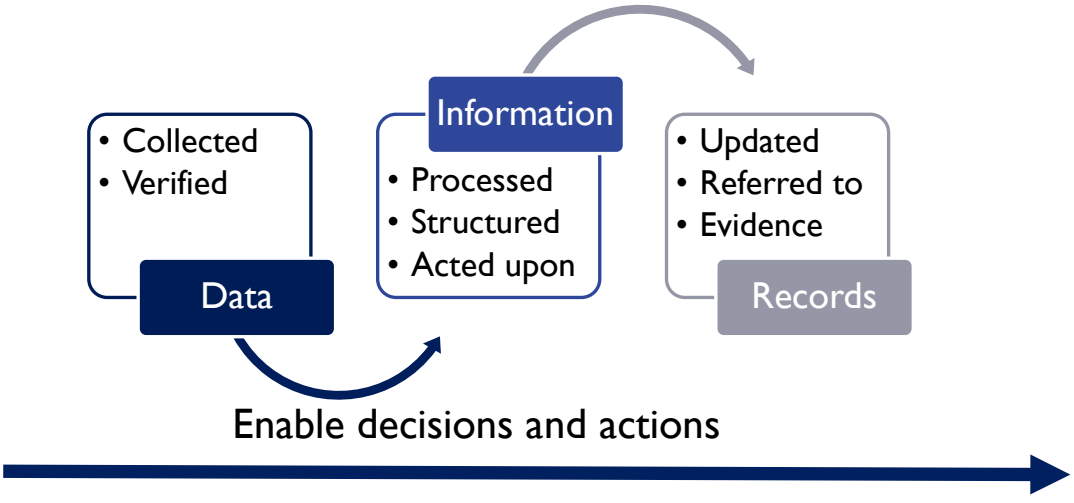
24 **Health records** consist of information and data relating to the physical or mental health or condition of an individual which have been made by or on behalf of a health professional in connection with the care of that individual.

25 **Social work records** include the records held by a Local Authority in connection with its social services functions under the Social Work (Scotland) Act 1968.

26 **Integrated care records** include information that is provided, accessed, updated, and relied upon, by multiple organisations. The agencies involved may use the records for different purposes, and they will have an arrangement(s) in place that sets out their different roles and responsibilities, including any obligations under the Public Records (Scotland) Act 2011 and the UK General Data Protection Regulation.

27 The Code of Practice adopts the approach with the Public Records (Scotland) Act 2011, Part 1 Section 13(1) which states that "record" means anything in which information is recorded in any form. Hereafter, any reference made to 'records' will be the overarching term used for all records, information and data held by health care organisations regardless of type and format. Of note this is also the approach taken in BS 10025[2].

Figure 1 – Data, Information, Records Process



[2] BS 10025:2021 | 30 Apr 2021 | BSI Knowledge (bsigroup.com)

28 **Records management** is the systematic control of an organisation's records, throughout their life cycle, in order to meet operational business needs, statutory and fiscal requirements, and community expectations. Effective management of corporate information allows fast, accurate and reliable access to records, ensuring the timely destruction of redundant information and the identification and protection of vital and historically important records.[3] (National Records of Scotland).

29 Records management forms part of the organisation's functions related to governance and assurance. It is the professional discipline associated with managing and governing data, information and records from the point of creation throughout the lifecycle to their final disposal. The activities include identifying, classifying, storing, securing, retrieving, tracking, archiving and destroying records. Fundamentally records management is concerned with knowing what information you hold, where it is and how long you are required to retain it, either in relation to business or regulatory/legislative requirements.

30 **Archive (noun)**, is a physical or digital collection of records of continuing value, either for historical research, corporate memory or accountability purposes. In the context of health care, records are generally transferred to an external archival facility, operated by the National Records of Scotland, a University, Local Authority or sometimes an internal archive. These facilities are referred to as a permanent place of deposit. An archive must meet strict operational and environmental standards in order to preserve and maintain the integrity, accessibility and availability of the records for a significant number of years or indefinitely.

31 **Archive (verb)** is used to describe the action of transferring records to an archival facility for permanent preservation. The term archive is often incorrectly used to describe the ongoing storage of 'inactive' records physically or digitally within an organisation without the appropriate preservation standards in place. Therefore this document will refer to 'transfer to the permanent place of deposit' rather than archive to be clear on the action being described/recommended.

32 **Data Sharing** is the process where information or records are shared between organisations (for example patient details provided by NHS to a Local Authority to progress hospital discharge) and that information becomes part of the records held and managed by the recipient organisation and the recipient organisation becomes the owner of their copy. The organisations may work together; however, they manage their records separately.

33 **Data Processing** is where information is processed on behalf of another organisation under contract. Records management arrangements should be outlined under contract when data processing agreements are entered into.

34 **Joint Data Processing** is where arrangements create a 'Joint Controller' relationship, and joint data processing, where information flows between organisations in a manner which is different to data sharing. This may result in joint records being created. Steps should be taken to ensure that all individual organisations document the arrangements in place so that records are managed in accordance with their relevant statutory obligations. An example of such

[3] Records Management | National Records of Scotland (nrscotland.gov.uk)

arrangements is the integrated services within Health and Social Care Partnerships which were created as a result of the Public Bodies (Joint Working) (Scotland) Act 2014.

2.2 Business Requirement for Managing Records

35 Records are vital assets of an organisation, and therefore it is essential that effective records management systems and practices are implemented.

36 Effective records management supports operational efficiency and delivery of services 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 digital space. It also supports better decision making and reduction in error when staff are accessing up to date, accurate and relevant information.

37 Records are a valuable resource because of the information they contain. High quality information underpins the delivery of first-class evidence-based care, accountability, governance, and many other key service deliverables. Information has most value when it is accurate, up to date and easily accessible when it is needed. Effective records management 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 to:

- support the delivery of 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/services users and customers or other individuals made through provisions of legislations;
- assist clinical and business 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/service user choice and control over treatment and services designed around them;
- support patient/service user safety and safeguarding;
- support accountability and transparency in the provision and management of services.

2.3 Regulatory Framework: Legal and Professional Obligations

38 This Code of Practice does not constitute legal advice. Organisations should consult their own legal advisors for advice on any legal issues that arise regarding the matters covered in this Code of Practice.

39 Organisations across the health and social care sector may be subject to the following legislation:

- Public Records (Scotland) Act 2011
- Access to Health Records Act 1990
- Freedom of Information (Scotland) Act 2002
- Environmental Information (Scotland) Regulations 2004
- UK General Data Protection Regulation/Data Protection Act 2018
- Inquiries Act 2005
- Network and Information System Regulations 2018/Scottish Public Sector Cyber Resilience Framework

40 Health and social care organisations and professionals have a common law duty of confidentiality to patients/service users. Their employees, contractors and volunteers also have a duty to maintain professional ethical standards of confidentiality; this duty continues after leaving the organisation. Obligations around confidentiality remain even after the death of a patient/service user.

2.3.1 Public Records (Scotland) Act 2011[4]

41 The Public Records (Scotland) Act 2011 (PRSA) places an obligation on named public authorities to:

- prepare, implement, and keep under review a Records Management Plan (RMP) which sets out proper arrangements for the management of their records (see Section 4.1);
- identify individual(s) who are responsible for management of the authority's records and for ensuring compliance with the plan;
- outline the procedures to be followed in managing the authority's public records, specifically around maintaining the security of information and the archiving and destruction or disposal of records.

42 Under Part 1, Section 3(1) of the Act public records are defined as:

a) records created by or on behalf of the authority in carrying out its functions,
b) records created by or on behalf of a contractor in carrying out the authority's functions,
c) records created by any other person that have come into the possession of the authority or a contractor in carrying out the authority's functions.

43 Named authorities are obliged under Section 3 of the PRSA to safeguard public records being created on their behalf by third parties when contracted to deliver one or more of a public authority's functions. An authority's expectations for the management of its public records created or held by the third party should be detailed within standard contract terms and conditions as required under Part 1 Section 3(1)(b) of the PRSA and Element 15 of the Keeper's Model RMP.

[4] Public Records (Scotland) Act 2011 (legislation.gov.uk)

2.3.2 Access to Health Records Act 1990[5]

44 The Access to Health Records Act 1990 provides certain individuals a right to see the health records relating to a deceased patient. These individuals are defined under section 3(1)(f) of that Act as:

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

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

- if there is evidence that the deceased did not wish for any or part of their information to be disclosed; or
- if disclosure of the information would cause serious harm to the physical or mental health of any person; or
- if disclosure would identify a third party (i.e. not the patient nor a healthcare professional) who has not consented to that disclosure;
- it applies only to records created on or after 1 November 1991.

46 It is important that organisations put processes in place to verify the identity of the applicant and have procedures to enable the efficient and effective retrieval of records within the timescales specified by the Act. Organisations should take steps to ensure that where required, consideration is given as to whether a medical professional is required to screen the notes before release.

2.3.3 Freedom of Information (Scotland) Act 2002[6] and Environmental Information (Scotland) Regulations 2004[7]

47 All records and information held by named public authorities are requestable under Freedom of Information (Scotland) Act 2002 (FOISA) and Environmental Information (Scotland) Regulations 2004 (EIR), subject to applicable exemptions. FOISA was designed to create transparency in Government and allow anyone to know about the provision of public services through the right to submit a request for information. EIR was designed to provide citizens with the right to request environmental information held by Scottish public authorities.

48 These rights are only as good as the ability of those organisations to supply information through best practice records management programmes. Under Section 61 of FOISA, Scottish Ministers have published a Code of Practice on Records Management for Scottish Public Authorities. The Code of Practice sets out the acceptable standards for the management of records to support compliance with FOISA. Under Regulation 4 of EIR there is a specific requirement on a public authority to take reasonable steps to organise and keep up to date environmental information relevant to its functions.

[5] Access to Health Records Act 1990 (legislation.gov.uk)
[6] Freedom of Information (Scotland) Act 2002 (legislation.gov.uk)
[7] The Environmental Information (Scotland) Regulations 2004 (legislation.gov.uk)

2.3.4 Data Protection Laws[8]

49 The Data Protection Act (DPA) 2018 is the principal legislation governing how organisations process and handle personal data, including special categories of data, such as health-related data. The UK General Data Protection Regulation and the Data Protection Act 2018 provide the legal framework[9] for processing personal data, including that contained within health and social care records. Records containing personal data must be managed in accordance with the requirements of this legislation.

50 The Data Protection Principles state that personal data shall be

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.

51 In addition organisations have an accountability principle which requires organisations to take responsibility for how they process and manage personal data and how they comply with the other principles.

52 The Act also provides exemptions with regards to Research and Statistics – Schedule 2 Part 6 Paragraph 27 and Archiving in the public interest – Schedule 2 Part 6 Paragraph 28(1). Further supporting guidance on archiving has been produced by The National Archives[10].

53 Handling records in a way that complies with these principles, as well as the many rights conferred on individuals by the legislation, is not only good records management, but is also necessary for data protection legal compliance.

54 Data protection legislation provides people with information rights over the health and social care data processed about them. However, controller organisations are obliged to consider the requirements of this Code of Practice when considering information rights requests made by citizens, in particular the right to object.

2.3.5 Inquiries Act 2005[11]

55 The Inquiries Act is intended to provide a comprehensive statutory framework for Ministers to set up formal, independent inquiries relating to particular events which have caused or have potential to cause public concern, or where there is public concern that particular events may have occurred. Of note:

[8] Data Protection Act 2018 (legislation.gov.uk)
[9] An overview of the Data Protection Act (ico.org.uk)
[10] Data protection legislation - The National Archives (nationalarchives.gov.uk)
[11] Inquiries Act 2005 (legislation.gov.uk)

- Section 21 of the Act provides inquiries with statutory powers to compel evidence.
- Section 35(1) of the Act makes it an offence to fail, without a reasonable excuse, to comply with a formal notice requiring attendance at the inquiry or the production of evidence. Subsections (2) and (3) go wider, making it an offence to deliberately distort or conceal relevant evidence.

56 The Inquiries Act 2005 is supplemented in Scotland with The Inquiry (Scotland) Rules 2007.

57 If an Inquiry is conducted, which covers health care organisations within Scotland, they must take action to identify and protect records which may be relevant to the inquiry. Records form an important part of the evidence in inquiries. What is required can vary by Inquiry; however organisations will need to consider what information may be relevant based on the terms of reference for the Inquiry. It is an offence to fail to provide evidence (which is held by the organisation) required by the Inquiry, therefore organisations must put in place the appropriate measures to ensure as far as reasonably possible that information and records are prevented from alteration or deletion and are easily retrievable should they be requested.

58 At the time of writing there are four independent Inquiries which impact on health and social care organisations in Scotland:

- Scottish Child Abuse Inquiry
- UK Infected Blood Inquiry
- Scottish Hospitals Inquiry
- UK Covid-19 Inquiry and the Scottish Covid-19 Inquiry

59 Other legislation requires information to be held as proof of an activity against the eventuality of a claim (e.g. Prescription and Limitation (Scotland) Act 1973 or the Consumer Protection Act 1987).

2.3.6 Network and Information System Regulations 2018[12] / Scottish Public Sector Cyber Resilience Framework (version 2)[13]

60 The Network & Information Systems Regulations 2018 (NIS Regulations) provide legal measures to improve the level of security (both cyber & physical resilience) of network and information systems for the provision of essential services and digital services. Scotland's devolved health and water sectors are legally required to comply with the NIS Regulations. In Scotland the main Operators of Essential Services (OES) are considered to be Scottish Water (with the Drinking Water Quality Regulator for Scotland as the Competent Authority) and all NHS Scotland Health Boards (with the Scottish Ministers as the Competent Authority).

61 All OES must comply with the standards set out in the NIS Regulations. These standards cover managing security risk, defending systems against cyber-attack, detecting cyber security events and minimising the impact of cyber security incidents. Complying with the standards includes the Health Boards reporting improvements to

[12] The Network and Information Systems Regulations 2018 (legislation.gov.uk)
[13] Cyber resilience: framework and self assessment tool (gov.scot)

resilience and capabilities to the Scottish Health Competent Authority (SHCA)[14] through NIS regulatory audits. In doing so, the SHCA is able to monitor continual improvements by NHS Scotland Health Boards against the 427 controls in the Public Sector Cyber Resilience Framework (PSCRF).

62 Local Authorities are currently **not** classed as OES under the NIS Regulations. So therefore aren't legally required to comply and don't report into any Competent Authority. However, they must comply with the PSCRF and look to achieve Tier 1 controls as a minimum. SG Cyber Resilience Unit carry out annual cyber surveys which includes all Local Authorities.

2.3.7 Professional Obligations

63 Staff who are registered to a professional regulatory body are required to adhere to record keeping standards defined by their registrant body. This is designed to guard against professional misconduct and to provide high quality care in line with the requirements of professional bodies. Further information about professional standards for records can be obtained from relevant professional bodies:

- General Chiropractic Council (GCC)
- General Dental Council (GDC)
- General Medical Council (GMC)
- General Optical Council (GOC)
- General Osteopathic Council (GOsC)
- General Pharmaceutical Council (GPhC)
- Health and Care Professionals Council (HCPC)
- Nursing and Midwifery Council (NMC)
- Scottish Social Services Council (SSSC)

64 Health and social care staff may also wish to consult the Professional Records Standards Body, which produces care record standards to improve the safety and quality of health and social care; and ensure that the right information is recorded correctly and can be accessed easily.[15]

[14] Scottish Health Competent Authority (healthca.scot)
[15] The Professional Record Standards Body - PRSB (theprsb.org)

Section 3 - Responsibilities

65 The records management function should be recognised as a specific corporate responsibility within every organisation. It should provide a managerial focus for records of all types in all formats, 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.

66 All individuals who work for an NHS Board, Local Authority or organisation contracted to deliver a service on their behalf are responsible for any records that they create or use in the performance of their duties.

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

68 **The Integration Joint Board** is responsible, for the strategic planning of the Health Board and Local Authority functions delegated to it and for ensuring the delivery of those functions through the directions issued by it under section 25 of the Public Bodies (Joint Working) (Scotland) Act 2014. The Integration Joint Board will also have an operational role as described in the locally agreed operational arrangements set out within their integration scheme[16].

3.1 Responsibilities

69 There are a number of records management responsibilities which should be allocated to roles within organisations. The following roles are examples of how the responsibilities can be allocated however the roles may have different titles and may not be allocated to separate individuals.

70 **The Chief Executive** has overall independent responsibility for records management. 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).

71 **The Senior Information Risk Owner (SIRO)** oversees the identification, assessment, and treatment of information risks within the organisation. Those are risks related to information and information technologies, including records and records management information systems. They should sit at director level or equivalent and must provide the Accounting Officer and Executive Board with assurance that information risk is being managed appropriately and effectively across the organisation and its services providers. Furthermore, they play a crucial role in recognising opportunities stemming from information and information technologies, thereby facilitating informed decision-making processes, and fostering a culture of innovation and growth driven by information and related technologies. This strategic position requires a comprehensive understanding of the organisation's objectives,

[16] Roles, Responsibilities and Membership of the Integration Joint Board (www.gov.scot)

coupled with the ability to align risk management, information and information technologies strategies with overarching business goals.

72 **The Caldicott Guardian** provides advice within health organisations regarding the ethical use of patient data and the application of the Duty of Confidentiality. They act as the “conscience of the organisation” reflecting patients' interests regarding the use of patient identifiable information.

73 **The Data Protection Officer (DPO)** holds a key advisory and monitoring role in relation to the use and management of personal data. Their role and responsibilities are defined under UK GDPR and Data Protection Act 2018. The key tasks all DPOs must undertake as part of their role includes:

- informing and advising the controller or the processor, and their employees, of their obligations under data protection legislation;
- monitoring compliance with the UK GDPR and other data protection laws, through implementation of data protection policies, managing internal data protection activities; raising awareness of data protection issues, training staff, and conducting internal audits;
- providing advice, where required, on data protection impact assessments and monitor compliance with this requirement;
- act as point of contact for the Information Commissioners Office (ICO) for matters relating to 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).

74 **The Records Manager** has the lead responsibility for the overall development and maintenance of records management within the organisation. They are responsible for embedding records management into day to day practices to support the delivery of services, compliance with legislation and the efficient, safe, appropriate, timely retrieval/disposal of records. They will:

- provide strategic direction and advice on matters concerning records;
- develop policies, guidance, and training at all stages of the records lifecycle - creation, use, maintenance, review and disposal;
- work closely with manager(s) responsible for other information governance work areas;
- work closely with colleagues within IT, ensuring that they are involved in projects regarding the development/implementation of new systems or the upgrade of current ones;
- work closely with colleagues involved in estate management with regards to the physical storage of records.

75 Within public authorities, this role will be responsible for the compliance with the Public Records (Scotland) Act 2011 and should be named at Element 2 of the organisation’s RMP as required under Part 1 Section 1(2)(a)(ii) of the PRSA. This role should be formally acknowledged, outlined in job descriptions, and communicated throughout the organisation.

76 Within a large organisation the Records Manager should be a designated member of staff of appropriate seniority, ideally with suitable records management qualifications. Within, for example a territorial NHS Board, the responsibility should be split into health records manager and corporate records manager.

77 Within a smaller organisation the role could be undertaken by a Care Home Manager or Practice Manager who could take on a records management lead capacity.

78 As records management activities are undertaken throughout the organisation, mechanisms must be in place to enable the records manager to exercise an appropriate level of management of this activity, even where there is no direct reporting line. This might include cross-departmental records and information working groups or individual information and records champions or coordinators who may also be Information Asset Owners.

79 **The Archivist** is 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 staff or users and identify relevant material of historical value ensuring transfer to a designated place of deposit for archival preservation. Note that valuable historical information may be 'born digital' and exist as digital files as well as traditional paper archives.

80 **The Information Asset Owner (IAO)** has responsibility for ensuring information assets (records) are processed in a safe, fair, and lawful manner. They are responsible for managing information risk associated to the Information Assets they are responsible for on behalf of the organisation and providing assurances to the SIRO. IAOs are senior individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the management, security and use of the assets. IAOs should recognise records management as a key aspect of most roles and ensure that staff have time and resource to manage records appropriately, including remedial work on their legacy records. In larger organisations, an IAO might be a department head, for example.

81 **All staff** who create, receive and use data, information 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 organisation. 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.

82 **The Processors and Subcontractors** processing data, information and records on behalf of health care organisations must abide by this Code of Practice. Subcontractors may also have their own direct recordkeeping responsibilities as service providers, employers and regulated bodies. Contracts and relationships with third parties must be managed so that other aspects of records management are protected. This includes data protection clauses, provision of clear instruction on

expected standards of recordkeeping, returning the data, information or records, or transferring the data, information or records to a new supplier to ensure continuity of service.

83 Data Protection Officers may advise on whether contractual arrangements in place with processors are appropriate and on whether further information must be added to relevant privacy notices.

84 Should a subcontractor close 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 as per Section 3 of the PRSA.

3.2 Training

85 All staff involved in handling records, should be appropriately trained in their records management responsibilities, and are competent to carry out their designated records management duties. Training should cover paper and digital record formats.

86 Public authorities have a duty to ensure the provision of training for staff regarding records management in support of their compliance with Element 12 of the Keeper's Model RMP, under PRSA. Specific elements should be included in training programmes to ensure staff understand appraisal and retention of records.

3.3 Policy

87 In support of their compliance with Part 1 Section 1(2)(b)(i) of the PRSA and Element 3 of the Keeper's Model RMP, public authorities should have in place a records management policy statement, endorsed by the Executive Management Team (or its equivalent), and made readily available to staff at all levels of the organisation.

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

89 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 those of individual staff to document 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 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;

- 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.

90 The policy statement should be reviewed at regular intervals (a minimum of once every three years or sooner if new legislation/codes of practice/national standards are introduced or due to obligations placed on organisations by their auditors) and, if appropriate, it should be amended to maintain its relevance. The policy should be ratified through the appropriate governance route within the organisation with final approval being provided by an appropriate senior group, for example the Information Governance Committee within a large organisation or by the senior executive team within a smaller organisation.

91 To support the implementation of the policy, organisations should develop local guidance outlining how records are managed within their organisation, including what they should contain, what format they should be held in, where they should be stored, what the file structure and naming conventions should be and the security measures which must be put in place to prevent inappropriate access.

Section 4 - Data, Information and Records Lifecycle Management

92 This section provides organisations with guidance regarding how to manage records throughout their lifecycle. As outlined in Section 2.1, this Code of Practice adopts the approach with the Public Records (Scotland) Act 2011 (PRSA), Part 1 Section 13(1) which states that "record" means anything in which information is recorded in any form. Here after, any reference made to 'records' will be the overarching term used for all records, information and data held by organisations regardless of type and format.

4.1 Records Management Plan/Framework

93 Section 1 of the PRSA requires every public authority to prepare a "Records Management Plan" (RMP), setting out proper arrangements for the management of their public records throughout its lifecycle.

94 The Keeper's Model RMP[17] provides public authorities with a framework to set out how their records are being managed. It is separated into 15 elements and each public authority is required to report on their status for each element to the Keeper of the Records of Scotland and provide evidence to demonstrate this. The elements are as follows:

Figure 2 Records Management Plan Elements

95 Health and social care organisations working within the private, third party or voluntary sectors should ensure that they manage the records in line with the contracting organisation's Records Management Plan.

4.1.1 ISO 15489 Information and Documentation

96 Organisations should refer to ISO 15489 Information and Documentation - Records Management Standard [18]which focuses on the business principles behind records management and how organisations can establish a framework to enable a

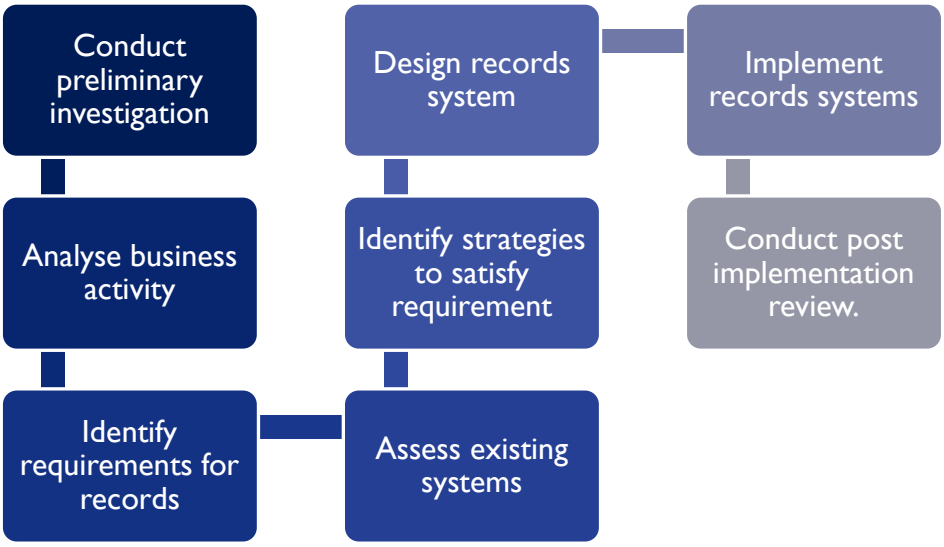
[17] Model Records Management Plan | National Records of Scotland (nrscotland.gov.uk)
[18] ISO 15489-1:2016 Information and documentation - Records management (iso.org)

comprehensive records management programme. This can be used to support the implementation of the organisation's Records Management Plan.

97 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. It is essential that a records management process is designed that will allow records to possess these characteristics. To ensure that these characteristics are maintained, sufficient persistent metadata (see section 4.7.2) must be attached to each record.

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

Figure 3 Implementation of record keeping process



99 In addition to the stages outlined above, in most cases an information risk assessment should also be conducted. The risk assessment should include identified privacy risks in compliance with the Information Commissioners Office Data Protection Impact Assessment Guidelines.

100 To support implementation of ISO 15489, the British Standards Institution developed BS 10025:2021 – Management of Records Code of Practice. It which sets out recommended good practices for organisations to follow, in the management of their records to support the implementation of principles detailed in ISO 15489 in practice.

4.2 Records Survey

101 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.) and how the records link to the organisational Business Classification Scheme. An information survey or

record audit is essential to meet this requirement to ensure control over the records and provide valuable data to inform future workplans and for developing records appraisal/disposal policies and procedures.

102 It will aid organisations to know:

- what series of records it holds (and potential quantities)
- the location of its records (outlining security/access measures)
- the format of its records
- the business area that created the record
- the information Asset Owner (responsible manager)
- disposal potential for the coming year.

103 The process can also be used as an opportunity to support asset owners with their records management responsibilities.

104 Organisations should annually audit their records management practices as part of its existing audit activity. This can include checking for adherence with this Code of Practice. Results of audits should be reported through the appropriate governance routes and updated on the organisation's RMP. For public authorities this is a requirement under Part 1 Section 5(1)(a) of the PRSA and Element 13 or the Keepers Model RMP.

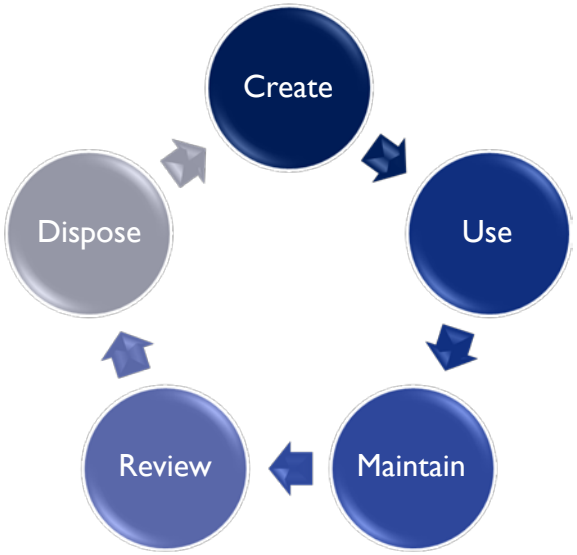
105 This audit must be extended to all organisations processing information on behalf of NHS Boards.

4.3 Managing Records

106 Records are required to be managed throughout their 'lifecycle'. This 'lifecycle' starts at creation or receipt of the record (information or data) in the organisation and continues throughout the period of its use, storage, review, and concludes with either confidential destruction or transfer to a designated place of deposit for archival preservation. All records in any format, (paper, digital files, emails, and data held within digital systems or databases) should be managed through each stage of the lifecycle regardless of whether its lifespan is a single day or a lifetime. Organisations should ensure that they have policies and procedures in place to manage records through each stage of the lifecycle, which supports compliance with Part 1 Section 1(2)(b)(i) of the PRSA and Element 3 or the Keepers Model RMP. The stages are shown in Figure 4 and described as follows.

107 **Stage 1 – Create**
This stage refers to the creation or receipt of records by an organisation. It is important that careful consideration is given to the purpose of the record, how it will be identifiable in the future, how long it will require to be retained and the storage and security measures required. At this stage, it may be possible to determine if the record needs to be defined as a master copy of a record. See section 4.5.

Figure 4 The Information (Records) Lifecycle



108 **Stage 2 – Use**
Stage two reflects the point at which the record is in active use by the organisation. Active use can refer to the records being updated regularly, being referenced, used in the delivery of services or to inform decision making. This may also involve sharing of this record with other functional areas or organisations. During this stage it is important that; the record is reviewed to ensure it meets its intended purpose, security/access is monitored to ensure it is only accessible by those who have a justified need to access, and version control is utilised to ensure points of change can be identified.

109 **Stage 3 – Maintain**
At this stage the record has fulfilled its intended purpose and becomes inactive, whereby the content is no longer altered but the record continues to be stored by the organisation. The record should be 'closed' (see section 4.11) and consideration given as to whether the retention period can be triggered. It is essential that the record is stored appropriately in order that: it continues to be visible to the 'owner', it can be identified when requested and it is managed through the final stages of its lifecycle. Access should continue to be monitored and any change to the storage or format of the record should be carefully considered. A further consideration is that at this point the records may be re-used for another purpose, for example for research, service improvement or as evidence in an investigation where a copy may be taken to form part of a new record.

110 **Stage 4 – Review**
At this stage of the lifecycle some records require to be reviewed and considered for continued retention, transfer to long term or offline storage, transfer to a permanent preservation facility or destruction. It is crucial at this stage that the 'owner' of the record has oversight of this decision making and that decisions are based upon business use, legislative requirements, and the organisations retention schedule. For some records, especially those in digital systems, automated deletion functionality may have been applied to appropriate record types which negates for the manual review of these record types. See 4.12 for further information.

111 **Stage 5 – Dispose**
The final stage of the lifecycle is the disposal of the record, either through transfer to the organisation's designated permanent place of deposit or by confidential destruction, so that the record is put beyond any possible reconstruction. Organisations should put in place robust procedures to ensure the secure and confidential destruction of records containing personal data. They should also record the disposal (destruction or deposit) of records on disposal logs and/or obtain destruction certificates where required, and particularly in the event of the destruction of personal data.

4.4 Creating Records

112 Organisational units/departments should have in place procedures for documenting their activities. This process should consider the legislative and regulatory environment in which the department operates.

113 At the point of creation, consideration should be given as to the purpose of the record and how it should be constructed in order to fulfil this purpose.

114 Records of organisational activities should adhere to the following records management principles as defined by the National Records of Scotland:[19]

Authentic	It must be possible to prove that records are what they purport to be and who created them, by keeping a record of their management through time. Where information is later added to an existing document within a record, the added information must be signed and dated. With digital records, changes and additions must be identifiable through audit trails.
Accurate	Records must accurately reflect the activities and transactions that they document.
Accessible	Records must be readily available when needed.
Complete	Records must be sufficient in content, context, and structure to reconstruct the relevant activities and transactions that they document.
Comprehensive	Records must document the complete range of an organisation's business.
Compliant	Records must comply with any record keeping requirements resulting from legislation, audit rules and other relevant regulations.
Effective	Records must be maintained for specific purposes and the information contained in them must meet those purposes. Records will be identified and linked to the business process to which they are related.
Secure	Records must be securely maintained to prevent unauthorised access, alteration, damage or removal. They must be stored in a secure environment, the degree of security reflecting the sensitivity and importance of the contents. Where records are migrated across changes in technology, the evidence preserved must remain authentic and accurate.

[19] Records Management | National Records of Scotland (nrscotland.gov.uk)

115 This is in order to:

- allow employees to undertake appropriate actions in the context of their responsibilities;
- facilitate an audit or examination of the organisation by anyone so authorised;
- protect the legal and other rights of the organisation, its patients, staff, and any other people affected by its actions;
- ensure the authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.

116 When creating and/or collating personal data in the formation of records, organisations must ensure that the collection of this data is necessary, justified, and proportionate, in support of data protection principles and therefore supporting compliance with Element 9 – Data Protection of the Keeper's Model RMP.

4.5 Defining Records

117 Within the organisation, there should be guidance to provide staff with a clear understanding of what constitutes a record and what records require to be kept. Organisations should adopt a master record approach, where a primary instance of the record is held. Master copies should be retained in line with the organisation's retention schedule. A master copy of a record should be managed in a way that will fix it in an accessible format until it is appraised for further value or disposed of, in line with the retention schedule. Some activities will be pre-defined as creating records which require to be kept, such as health records or minutes and papers of board meetings. Other records will need to fulfil the criteria as being worth keeping, such as unique instances of a business document, emails, or datasets.

4.5.1 Duplicate Records

118 Duplicate copies of records should be marked as such (preferably with the identification of the original IAO) to prevent being used as a master record in error. Copies of records are not usually required to be retained in line with the original retention period. They may be able to be held for a short period of time and disposed of once the business purpose for the record has ceased. However in some cases they may subsequently form part of a different record type, for example evidence in an investigation file or as part of a multi-agency record, and may require to be retained for longer.

119 Where data is duplicated, either due to data warehousing 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 are applicable to any record regardless of format.

4.5.2 Transient Information

120 Transient information is that which is deemed to be temporary, superseded or of little value, which would not be declared as a record itself. Examples include:

- A blood pressure results written on a post-it note which is transferred into the digital patient health record (superseded);
- A telephone message passed from one staff member to another (temporary);
- A draft document superseded by a final version (superseded);
- An email outlining that someone will be late for a meeting (temporary);
- Notes in a paper or digital notebook (temporary);
- Communications making arrangements for lunch (little value).

121 This information once transferred to the appropriate record, acted upon, or superseded should be held for a minimum amount of time, if at all. Individual employees do not need formal authorisation (from the IAO or line manager) to destroy transient information, so long as the records are not needed for an investigation or to respond to a request for information and the destruction is carried out in a secure manner. However, employees sometimes need help in determining whether information is transient or not and such queries should be referred to the organisation's Records Manager.

122 Transient information can be in paper or digital format. Across organisations there are a range of digital portals. These technologies generate transient records which are still subject to records management and information governance, particularly in terms of security measures and access controls. Any decisions made in relation to health and social care interactions using information that is accessed from digital portals must be recorded within the health or social care or social work record. Audit Logs showing the information/documents that were accessed must therefore be retained.. If transient information is recorded on hard paper copy the information must be transcribed into the record before the paper version is destroyed.

4.6 Registering Records

123 Organisations should maintain a register of information assets, commonly known as an Information Asset Register (IAR). It should contain details of the records (regardless of format) stored and maintained by the organisation, including any risks associated with them and should be reviewed annually.

124 Assets should be registered at record collection level. Information Asset Registers should contain the following details of each asset:

- the name, purpose and description
- the IAO and Information Asset Administrator (IAA)
- its format, location and the security applied
- its corresponding function in the Business Classification Scheme
- the retention period which should be applied
- any identified risks and mitigations.

125 When creating a new type of record, an initial information risk assessment should be conducted in conjunction with those responsible for records management information security and data protection. An IAO should be designated and they are responsible for conducting the information risk assessment. Any new information asset (e.g. a new type of record) should be registered. Of note one single system may have more than one information asset with different IAOs, e.g. clinical data vs. operational logs may have different IAOs.

126 The UK General Data Protection Regulation (UK GDPR) requires organisations to maintain a record of processing activities (ROPA) under its responsibility. This also fulfils part of the requirements under Element 9 – Data Protection of the Keeper's Model RMP. The ROPA can be linked to or detailed within an Information Asset Register providing it contains details of the information processed by the organisation (digital or otherwise), the sensitivity and classification, the information risk, groups of users and who the information is shared with.

4.7 Identifying Records

127 Records must be easily identifiable using naming conventions and metadata. The naming or labelling of digital or paper files must clearly identify the contents of the file, the time period which it relates to and the version number where applicable. Information Asset Registers should allow the identification of IAOs.

4.7.1 Naming Conventions

128 Organisations must have guidance for naming conventions of digital records (files and folders); this helps identify records 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.

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

130 National Records of Scotland guidance states: "A document name should be made up of the following components:

Description - the topic and subject matter. This component may be used numerous times as documents are created and saved relating to the same subject. This should adequately describe the contents out with the folder structure.

Type - the document type e.g. letter, report, minutes, etc. Not to be confused with format e.g. Excel spreadsheet

Date, if appropriate - the date of, publishing/approval, or of an event, meeting and used to distinguish the document from others on the same topic. The most practical format for dates is YYYY-MM-DD or YYYYMMDD as per ISO8601[20] Date and Time Format. This allows for easier searching and sorting.

Version Number - used to keep track of changes made to the document. Not applicable to emails."

[20] ISO 8601 Date and time format (iso.org)

4.7.2 Metadata

131 Metadata is structured information that enables us to describe, locate, control, and manage other data/information/records throughout its lifecycle. 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 descriptive metadata about the book but is not the book itself.

132 Organisations should therefore ensure that metadata includes as a minimum, elements such as the title, subject and description of a record, the creator and any contributors, the date and format. For patient health records, organisations must also ensure that they use the appropriate DST Code as outlined within the Scottish Clinical Indexing Standards[21] and the patient's CHI number where appropriate.

133 The UK Government Central Digital and Data Office states within its Metadata Standards for Sharing and Publishing data guidance[22] that the Open Standards of Schema.org[23] and Dublin Core[24] that are both recommended for government[25] use.

4.7.3 Version Control

134 Organisations should include details of the current and previous versions of the record in the metadata and/or using naming conventions for such purpose. Appropriate version control arrangements that support the management of multiple revisions to the same document should be in place, to ensure that the most up to date versions are being referred to by staff or to ensure that the record which was in place at a certain point in time is easy to identify. To assist with version control for an organisation's controlled documents e.g. policies, guidelines, procedures, it is recommended that document control forms are also in place, which detail the version history and changes applied. Some systems automatically generate version histories for example within SharePoint; however, this can result in a new version being 'logged' each time a change is made and may not reflect the version history for long-standing documents which have been migrated into the system.

4.8 Storing Records

135 Records created by organisations should be arranged in a record management system that will enable the organisation to obtain the maximum benefit from the quick and easy retrieval of records whilst also having regard to security frameworks.

136 Paper and digital record management systems should include descriptive, contextual, and technical documentation and metadata to enable the system to be operated efficiently, and to allow the records held in the system to be easily understood. It

[21] Clinical Indexing Document Standards v4.3 (digihealthcare.scot)
[22] Metadata standards for sharing and publishing data - UK Gov (gov.uk)
[23] About Schema (schema.org)
[24] DCMI Metadata Terms (dublincore.org)
[25] UK Gov e-Government metadata standard v3.1 (nationalarchives.gov.uk)

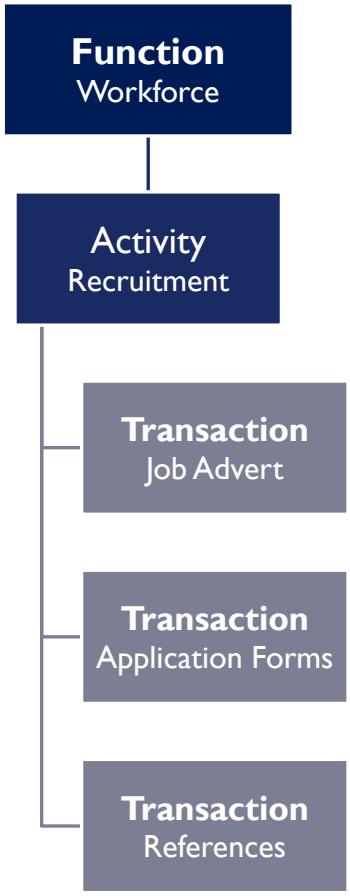
should be clear from this documentation the administrative history and context of the records. The systems should also enable clear rules for the labelling and protective marking of records to maintain security and confidentiality, whilst aiding efficient record retrieval.

4.8.1 Structuring Records

137 Records should be structured within an organisation-wide corporate 'file plan' or Business Classification Scheme which reflects the functions and activities of the organisation and facilitates the appropriate sharing and effective retrieval of records. This supports the organisation's requirements under Element 4 of the Keeper's Model RMP and the requirements of ISO 15489.

138 The Business Classification Scheme can be implemented as the structure of files and folders in a paper filing system, on a network shared drive or as metadata/labelling/tagging within an Electronic Document and Records Management System (EDRMS). Classification schema should be structured by function and then further refined to produce a classification tree based on function, activity, and transaction. The transaction can then be assigned a rule (such as retention period), a security status or other action based on the organisational policy. The scheme will enable appropriate management controls to be applied and support more accurate retrieval of information from record systems. A Business Classification Scheme should not be based on organisational/departmental structure as this is subject to periodic change.

Figure 5 Business Classification Scheme



4.8.2 Securing Records

139 Records must be stored in a secure environment to prevent unauthorised access, alteration, damage, or removal. The level of security should reflect the sensitivity and importance of the information.

140 Information Security, Element 8 of the Keeper's Model RMP, is a compulsory element under Part 1 Section 1 (2)(b)(ii) of the PRSA. Organisations must ensure that they have appropriate measures in place to protect information and be able to demonstrate this in evidence.

141 The 6th Data Protection Principle detailed in Article 5(1)(f) of the UK GDPR requires organisations to take reasonable technical and organisational security measures to protect information from unauthorised access, unlawful processing, accidental loss, destruction, or damage.

142 The Public Sector Cyber Resilience Framework supports Scottish public sector organisations to improve their cyber resilience and comply with a range of legislative, regulatory, policy and audit requirements in respect of cyber security. NHS Boards specifically also have to comply with Network and Information Systems Regulations 2018.

143 It is recommended that organisations implement a protective marking scheme. This could, for example be based on the Cabinet Office Government Security Classifications defined protective marking scheme which is used by both central and local government. It is best practice that patient/service user data is classed as 'Confidential'. For those organisations implementing Microsoft 365, this could be implemented within the 'Sensitivity Label' functionality.

144 The paper records management system in place in most organisations is not necessarily an appropriate model for managing digital records. This is because of the nature and volume of digital records, the variety of file formats, the distribution of the storage and duplication (e.g. parallel datasets), the way it is backed up and preserved, and the difficulty to implement retention policies (unless they are embedded in the initial digital infrastructure) must be considered when securing digital records.

145 Digital records management needs to be very carefully considered and structured to ensure the integrity of the records is not compromised upon capture and during storage, so that data remains accessible and understandable for as long as it is required.

146 User access controls provide essential mitigation against the risks to records inherent in many digital systems. These controls include user registration and de-registration, user access provisioning, review of user access rights and the removal or adjustment of access rights. They also include the prohibition of shared accounts and access to information based on a need-to-know basis. Organisations must implement, where possible, monitoring systems to allow automated escalation of access misuse to digital records.

4.8.3 Accessing Records

147 Organisations should have processes, procedures, and technical controls in place to support the business continuity of records to ensure they are readily available when needed. This can be as simple and straight forward as ensuring that users do not store records in places which are not accessible to others; for example their computer desktop or electronic personal drive/OneDrive, or a locked filing cabinet, and can range to organisations having IT disaster recovery plans and back up processes to support the creation and management of records which are required for the operational delivery of services. Organisations are required to detail the measures in place under Element 10 of the Keeper's Model RMP.

148 Organisations should also ensure that the appropriate access controls are applied to records to ensure that they are not inappropriately accessed. This is particularly important where the records contain business sensitive or personal data. Organisations should ensure that IAOs are aware of their responsibilities in this area and that access controls should be reviewed on a routine basis.

4.8.4 Paper Records Storage

149 It is essential that paper records are stored in the correct environment. Guidance on the requirements can be found in BS 4971:2017 Conservation and care of archive and library collections. Environmental factors can have a significant impact on the structural integrity of the record and could result in significant damage to the paper which could result in the record being unreadable or damaged beyond use.

150 The following factors must be considered when identifying suitable storage for paper records:

- Accessibility to easily identify and retrieve records;
- Security measures to prevent unauthorised access;
- Ability to control environment to prevent against pests, excessive heat/light, mould, dirt, and damp;
- Flood/water ingress prevention;
- Fire protection.

151 Organisations should ensure that appropriate shelving is put in place, as well as identifying suitable packaging and labelling materials which are not subject to deterioration if required for long term storage.

152 Clear guidelines/procedures should be put in place to ensure that departments hold inventories of what records is contained in the storage area. The procedures should also outline the requirement for easy identification of records for disposal via the use of labels which clearly identify the:

- content owner (generally a department/team rather than a person);
- content subject matter;
- date of creation;
- date of destruction or requirement to retain permanently;
- box/file reference number.

4.8.5 Digital Records Storage

153 Where records are kept in digital 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 for the Management of Electronic Documents and Records (MoReq2)[26].

154 Where an EDRMS is not yet available, digital records should be stored on organisation approved shared network servers or Microsoft SharePoint in a clear and meaningful folder structure. The folder structure and/or associated metadata should reflect the organisation's file plan or Business Classification Scheme, which represents the functions and activities of the organisation. The server should be subject to frequent back-up procedures in line with the Public Sector Cyber Resilience Framework/NIS Regulations 2018. Users should apply the functionality of the relevant software to protect digital records against inappropriate amendment. Of note, it is almost impossible to fully protect documents in a non-EDRMS environment or provide full audit and authenticity evidence.

155 Cloud-based solutions are increasingly being implemented across organisations. The ICO cloud storage guidance must be followed and a data protection impact assessment must be conducted. Where possible, organisations should seek to ensure that their records, especially those which are sensitive, are stored on cloud-based solutions which have servers within the UK. Important considerations are:

- best practice records management must be applied, regardless whether 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.

4.8.6 Long Term Storage

156 Where records have been identified as inactive and have been closed, in some circumstances, it may be required to move them to long term storage within the organisation until they reach the retention period. This can be due to storage capacity/costs, the requirement to keep them secure or the requirement to protect their authenticity and integrity.

157 The transfer of records to long term storage should only be considered for records which have long retention periods and are not suitable for transfer to a designated place of deposit. For paper records this could mean moving the files from a filing cabinet into boxed storage within a dedicated record store. For records in digital systems this could mean moving the records from a legacy system into a supported platform. When moving digital records, there can be a greater risk to the integrity of the records of moving it than leaving it in situ. This should be considered and file fixity checks carried out for integrity and authenticity of records. The organisation's Records Manager should be involved in these projects.

[26] MoReq2 Overview (joinup.ec.europa.eu)

4.8.7 Offsite Storage

158 It is vital to highlight the importance of actively managing records which are stored in offsite storage. This applies to both paper records and digital records stored in cloud-based solutions. Organisations should ensure:

- IAOs are identified for the records as with any others, and to work in conjunction with Records Managers to commission new off-site storage – and DPOs for new processing of personal data;
- IAOs work with Records Managers to commission new off-site storage;
- DPOs are involved in commissioning processes where personal data is being processed and a Data Protection Impact Assessment (DPIA) is conducted to document this;
- there is a full inventory of what is held offsite;
- an entry is included in the organisation's IAR for the record set;
- retention periods are applied to each record;
- a disposal log is provided;
- there is evidence of secure disposal of records;
- they provide clear instructions relating to all processing of offsite records including destruction of the records;
- they can access the storage facility to conduct the appropriate checks when required;
- they have agreed how their records will be retrieved and what timeframe they will be returned, for example to respond to subject access and FOI requests;
- where suppliers/contractors are being used, they are subject to regular monitoring, including at contract reviews as part of healthy supplier relationship management.

159 The National Archives has produced guidance to support organisations with the considerations which need to be taken into account when sourcing offsite storage for paper records. It can be accessed via: Identifying and Specifying Requirements for Offsite Storage of Physical Records.

4.9 Digitising Records

160 Wherever possible, organisations should move to digital records. Although the original paper record guarantees the authenticity of the record, access can be more difficult to audit, there are physical storage implications and the records can be harder to access and share in a timeous manner. However organisations should also be mindful that although there is a cost-saving element associated with digitising records, equally, saving all digital records with no records management controls in place will similarly incur costs and is environmentally unsustainable.

161 Where possible, digital records management processes should be as environmentally friendly as possible to help contribute towards the Scottish Government's target to reduce its carbon footprint and environmental impact. An example would be to replace outdated IT servers with up-to-date energy efficient systems, reducing the amount of energy required for the solution.

4.9.1 Digitisation

162 Digitisation is the conversion of analogue (paper) to digital format. Digitising records may provide an opportunity to:

- increase efficiency;
- improve service delivery;
- enhance reporting;
- reduce storage space;
- reduce costs.

163 Organisations can digitise records by scanning current records into a digital storage solution or system. They should put in place robust procedures to manage control of access, retrieval, and use of records to ensure continued integrity, reliability, and authenticity of the records as well as their accessibility for the duration of their retention including the time of their disposal or archival preservation.

164 The key considerations an organisation should take into account when digitising records are:

- What information needs to be digitised and why?
  Should the records be securely destroyed without being digitised? Do all records require digitisation or just current or active files? There needs to be a clear rationale for digitisation, such as business efficiency, reduction of storage space or improvements in service delivery.

- Are the records suitable for digitisation?
  Consider the size and condition of the paper records; how large are they and how the digitised files will be used. For example, would it be feasible for someone to scroll through pages of scanned information to locate what they need without keyword searching? For example, for large files such as patient health records, it is advisable to scan into distinct sections that reflect the paper record structure.

- Who will own/manage the records once digitised?
  Information Asset Owners for the records should be identified. It is essential that ownership of the records is outlined to ensure that staff are aware of their responsibility to continue to manage the records.

- How will the records be quality checked?
  All digitised records should initially be quality checked, but the number that should be checked can drop incrementally over time. A minimum number, e.g. 5% of digitised records should always be quality assured to ensure:

  - Completeness (have all pages been scanned);
  - Legibility (can the pages be read/interpreted. Any issues with quality should be noted to indicate original condition; this can be done by utilising poor quality stamps or set scan sheets that state the digitised records are reproductions from poor quality originals);
  - Accuracy (is the digitised image an exact replica of the original document);

  - Legal admissibility (in accordance with BS 10008: 2020 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically: 1 & 2).

- Where will the records be stored?
  Consideration is required as to whether there is sufficient space to store large files; will more files be added in the future, and how much more storage will be needed.

- In what format will the records be stored?
  Organisations should consider the format in which the records will be stored in the digital solution. For example, PDF/A is specifically designed with long term preservation in mind.

- How will the records be identified?
  Organisations should consider what details should be required for the naming convention and/or metadata. They should also consider where the tagging functionality is supported and what tags could be applied alongside naming conventions and metadata to support the quick and accurate identification of information. Where possible it is important that standardised naming conventions/metadata/tagging are applied to specific record types: for example the Scottish Clinical Document Indexing Standard[27] for health organisations.

- How long should the records be retained?
  Paper copies should be kept for a minimum of three months following scanning so that any errors identified through quality checking processes can be rectified. The digitised record takes on the role of master copy and will be then subject to the relevant retention period as outlined in the organisation's retention schedule. Once digitised and stored, the records will need to be managed in line with records management principles and the records lifecycle (see section 4.3 and 4.4).

- Have information risks been assessed?
  For example, has a risk assessment or Data Protection Impact Assessment been undertaken?

165 The Institute of Health Records and Information Management (IHRIM) have produced guidance that can be useful for organisations considering scanning clinical records.[28]

4.9.2 Digitalisation

166 Distinct from digitising, digitalisation refers to the transformation of business processes or transactions through the use of digital technologies. This could also include the development of new systems or processes or the migration of existing data to a new system or platform.

[27] Resources - Digital Healthcare Scotland (digihealthcare.scot)
[28] Institute of Health Records and Information Management Guidelines (ihrim.co.uk)

167 Examples include:

- meetings held remotely by video conference;
- self-service check ins;
- data entry via online form directly into a system;
- implementation of a new clinical system.

168 When records are being moved from one system to another then it is likely that the structures used for the two systems will be different. To minimise risk to the records, organisations should gain an understanding of the following:

- The export and import functionality of both systems.
- The ways that metadata is captured and managed in both systems.
- File and object capture and management across both systems.
- Relationship management between objects, files, metadata, and other record-related relationship management across both systems.
- Any information types or formats that the decommissioning system has which cannot be captured or managed by the other system.

169 In cases where the processing of personal data is involved, a DPIA will be required. To ensure that any impact to records created, used, accessed, or stored by the proposed system or migration, it will be necessary to consider the following:

- Risk
- Ownership
- Record type
- Volume
- File format
- Security/access
- Retention/disposal
- Back-up/recovery
- Source of information
- Link to other information
- Information structure
- Information sharing
- Migration
- Data mapping
- System testing
- System decommissioning

4.10 Sharing Records

170 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 2.3 Regulatory Framework: Legal and Professional Obligations.

171 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.

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

173 Information Security staff should be able to advise on appropriate safeguards. The NIS Regulations and the PSCRF set out the requirements for the safe handling and transmission of records, across a range of media.

174 Modern digital records may have very complex and distributed architectures. Nevertheless, the organisation must be able to comply with current legislation, regardless how distributed the records are. 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 personal rights in a smooth manner along the data flow.

175 Organisations must ensure that they have robust procedures/agreements in place for the sharing of information and that this is clearly documented. They should clearly consider the implication of information sharing on records management and, where personal data is concerned, must take privacy and data protection into account to ensure that sharing is appropriate, safe, and secure. This supports the organisation with Element 14 – Shared Information of the Keeper's Model RMP.

4.11 Closing Records

176 Records should be closed, i.e. made inactive as soon as they have ceased to be in active use. An indication that a file of paper records or folder of digital 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. The date of 'closure' can be the trigger for the start of the retention period, i.e. closure of investigation, completion of action plan.

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

4.12 Reviewing Records

178 Reviewing records, also known as 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. To support staff with the review of records, organisations should put a retention schedule in place, outlining the time period which each record should be retained for – see section 4.14.

179 In some cases the deletion of digital records may be automated within a system or platform such as Microsoft 365, negating the requirement for a review. This would only be applied to records where it is appropriate to set deletion at the end of a retention period without the requirement for further review by a person. However functionality should be put in place to enable organisations to prevent the automated deletion in circumstances when the records require to be retained for longer, for example in the event of investigations or public inquiries. Robust procedures are also required in order to inform information asset owners of circumstances where records require to be retained for additional purposes.

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

Retain: records may need to be kept for longer than the retention period due to ongoing administrative and or clinical/care 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 longer period, the internal retention schedules will need to be amended accordingly and a further review date set. Otherwise, one of the following will apply:

Transfer: to the organisation's designated place of deposit or consult an 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 Part 1 Section 1(2)(b)(iii) of the PRSA and Element 7 or the Keepers Model RMP. Organisations that do not have their own archivist should consult an NHS/Local Authority 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/care need, and they have no long term historical or research value.

181 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.

182 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.

183 Organisations should ensure that they have mechanisms in place to identify records, containing personal data, for which the appropriate retention period has expired, in line with the 5th data protection principle detailed in Article 5(1)(e) of the UK GDPR. It is acknowledged that organisations will have different mechanisms available to them to achieve 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.

184 It is important, when reviewing records or setting automated retention in systems, that the long term historical and research value of the records are taken into account. Support can be sought from the organisation's identified Archivist as per Element 7 of the Keeper's Model RMP. Records which document the history and development of

the organisation and important policy decisions should be considered for archival preservation. In addition, samples of health records and older registers and ward journals may be valuable for historical medical and social research. Note that no surviving personal health or administrative record dated 1948 or earlier should be destroyed.

185 Records 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):

- Board and major Committee minutes;
- Annual reports and accounts;
- Policy and strategy documents;
- Significant departmental reports, reviews, and investigations;
- A change to policy or procedure for delivery of care;
- National public interest;
- 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.

186 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 available within the Keeper's Model RMP Guidance to Element 7.

187 It is expected that only a small proportion of records will require archival preservation however, appraisal before transfer is essential. For these purposes public authorities should have procedures and staff guidelines in place, written in consultation with the archivist from the designated place of deposit named in Element 7 of the Keeper's Model RMP as required under Part 1 Section 1(2)(b)(iii) of the PRSA.

4.13 Disposing of Records

188 It is particularly important that the disposal of records – which is defined as the point in their lifecycle (stage 5) when they are either transferred to a permanent place of deposit for preservation 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 master copies of records should be clearly documented on a records destruction/transfer log and approved by the appropriate Information Asset Owner.

189 Organisations should develop and implement a retention and disposal policy. The policy should be supported by, or linked to, the retention schedules (see section 4.14), and should cover all records created.

190 Staff in the operational area that ordinarily use the records will usually be able to identify records for disposal and/or destruction, which should be approved by the manager responsible for the area. 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. Where possible, the process of appraisal, review and disposition should be automated, removing the need for staff to undertake the manual review of complex sets of records.

191 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. For example within a health organisation, clinicians have a responsibility to identify any health records that they would like to be retained longer and this extension needs to be clearly indicated on the patient record system or paper files.

4.13.1 Transfer to Designated Place of Deposit (Archive)

192 Once records are no longer in use by an organisation, have no ongoing administrative value but have, or may have, long term historical, research or corporate memory value they should be selected for archival preservation. They should be transferred to a or designated place of deposit/archive once the business need or retention period has expired. This is a compulsory element under Part 1 Section 1(2)(b)(iii) of the PRSA and is covered within Element 7 – Archiving and Transfer Arrangements of the Keepers Model RMP. Organisations that do not have their own archivist should consult a Local Authority/University Archivist or the National Records of Scotland for advice.

193 Organisations should ensure that they have appropriate processes in place to transfer records of historical value. For health organisations, see sections 5.2 and 5.6 for further information on sampling patient health records for archival preservation.

194 When transferring records containing personal data, organisations must consider a living person’s data protection and confidentiality rights. Data protection legislation contains explicit provision for archiving purposes in the public interest as detailed in the Data Protection Act 2018 Schedule 2 Part 6, Paragraph 28. Organisations should inform archives of the period of time for which records containing personal data should not be available for access by the public, to ensure the data protection rights of the individual are upheld.

195 Best practice suggests that non-active records selected for archival preservation should be transferred as early as practicable and no later than 30 years from creation of the record, with digital records being transferred within a shorter period due to their inherent vulnerability to change or deletion.

196 Organisations should ensure that they have identified points of contact who coordinate the transfer of records. A process for the transfer of records should be agreed by both the organisation and place of deposit. It is also good practice to have transfer registers in place to ensure the organisation has oversight of their deposited records.

4.13.2 Destruction

197 Records (including copies) not selected for archival preservation and which are no longer required due to statutory requirement or administrative or clinical need should be destroyed in a secure manner appropriate for the level of confidentiality or protective markings they bear. This must be approved by a manager and can be undertaken on site or via an approved contractor. Destruction processes and procedures must be clearly defined and documented within the organisation as required under Part 1 Section 1(2)(b)(iii) of the PRSA and Element 6 or the Keepers Model RMP.

198 Confidential records should be destroyed in accordance with BSEN 15713:2023 - Secure Destruction of Confidential Material – Code of Practice. It is the responsibility of the 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 for paper, hardware and digital systems. There is a common law duty of confidence to patients, service users 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 organisation. Obligations around confidentiality remain even after the death of a patient/service user.

199 It is important to have destruction policies for digital records. The ability to retrieve deleted digital 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. Organisations should put processes are in place to ensure that digital records are destroyed beyond any reasonable reconstruction on hardware. With regards to software, record should be destroyed to the point where they are not retrievable by the user and only retrievable by IT staff within back-ups for a short period of time. Back-ups are for the purposes of business continuity/disaster recovery only, not a ‘just in case’ and therefore should also be purged of destroyed records within an appropriate timescale. If hardware or software is to be discarded, advice must be sought from the relevant IT/Cyber Security Officer.

200 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;
- format of record;
- date of destruction;
- who authorised destruction (Information Asset Owner;
- who carried out the process;
- reason for destruction (this should refer to the retention/disposal policy).

201 Disposal schedules would constitute the basis of such a record.

202 Whenever health records are being destroyed, this should be done with the necessary arrangements made to protect patient confidentiality where appropriate. 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 at a later date, make a Subject Access Request or other request for information. It is important that records of destruction of health records contained in this retention schedule are retained permanently. No surviving health record dated 1948[29] or earlier should be destroyed.

203 Personal health records should not be destroyed before the end of the period stated in the Code of Practice Retention Schedule. These periods reflect the statutory time limits for legal action to be brought.

204 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 organisation has decided not to disclose the information, until the complaint and appeal provisions of the Freedom of Information (Scotland) Act 2002 (FOISA) have been exhausted or the legal process completed. It is important to note that section 65 of FOISA, Regulation 19 of the Environmental Information (Scotland) Regulations 2004 and Section 35(1) of the Inquiries Act 2005 detail that it is a criminal offence to destroy records with the intent to prevent disclosure.

205 Data Protection legislation requires the 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.

206 In complex settings where the information is shared and maintained across different organisations, the retention period should ideally be consistent. Where this is not the case retention periods should be aligned to the longest retention period for that record type specified in the sharing organisations records retention schedule.

207 When digital systems are being designed, thought should be given as to how records can be destroyed within the system. In circumstances when automatic destruction functionality is implemented on a system, the system must also have the ability to place legal holds on records which may require to be retained beyond the defined retention period, for example due to an ongoing investigation or public inquiry.

208 Where a digital 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 retention schedule should be followed in the same way for digital records as for paper records.

209 Specific management software may be required to allow automated disposal of digital records. Retention schedules are based on the legal, regulatory or business requirement for retaining information, hence the format (paper or digital) should be irrelevant. However this is a very difficult process and currently presents great

[29] MEL(1993)152 Guidance for the Retention and Destruction of Health Records (scot.nhs.uk)

challenges for organisations, particularly in relation to health records, where due to the dynamic nature of these records a different approach can be required. 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 organisation's records retention schedule.

210 Whilst there is a recognition that efficient disposal management is very difficult using legacy systems, organisations must demonstrate that disposal management is embedded in their change management processes; data protect by design and by default is a requirement for all organisations processing personal data (UK GDPR). Failure to demonstrate reasonable steps will constitute a breach of data protection legislation.

211 If the system does not have this capacity, then once the records have reached the end of their retention periods, they should be exported and destroyed. Where this is not possible they should be made inaccessible to users of the system and upon decommissioning the entire system should be retained, along with system audit trails, for the retention period of the last entry recorded in the system.

4.14 Retention Schedule

212 A retention schedule sets out the periods for which the various records created within the organisations should be retained either due to their on-going business 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 the designated permanent place of deposit. The implementation of a retention schedule is a requirement under Element 5 – Retention Schedule, of the Keeper's Model RMP. It also supports principle 5 of data protection legislation.

213 Schedules should cover all record types within the organisation, 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 should be based on the retention schedules referred to above, for the organisation. Retention schedules do not provide specific guidelines on determining which documents are retained as part of a record.

214 The baseline retention schedule followed by Local Authorities and third party organisations contracted by them to deliver services on their behalf in relation to social care and social work services has been developed and is maintained by the Scottish Council on Archives. The Scottish Council on Archives Records Retention Schedules (SCARRS) is used by Local Authorities to inform their own record retention schedule, and local adaptations may have been made to suit the operations of the organisation.

215 The retention schedule enclosed within this Code of Practice (Annex B) provides information and advice about all records commonly found within NHS organisations or third party organisations working on their behalf to deliver health care. The retention schedules apply to all the records concerned, irrespective of the format (e.g. paper, databases, emails, X-rays, photographs) in which they are created or held.

216 Whenever the enclosed schedule (Annex B) is used, the guidelines below should be followed:

- The retention periods in this schedule should be adopted. Local business requirements or risk analysis may require some record types to be retained for longer; however, they must never be retained for a shorter retention period than set out in this schedule.

- Retention periods should be calculated from the suggested trigger point.

- The provisions of the FOISA and data protection legislation must be observed. Retention decisions should be made 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 record must be permanently preserved and the advice of the NHS Board/Local Authority designated archivist or National Records of Scotland or the Scottish Government Digital Health & Care Directorate regarding the designated permanent place of deposit should be sought. This is a requirement under Part 1 Section 1(2)(b)(iii) of the PRSA and Element 7 of the Keepers Model RMP.

- 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 exportation, deletion or destruction is not technically feasible, due to the age and legacy design of the system, the record should be made permanently inaccessible to all reasonable measures, e.g. deleting encryption keys for that record. The organisation may wish to consider raising a risk in these circumstances due to the impact of retaining information (particularly personal data) for longer than is necessary, for example:

  - Compliance with the 5th principle of data protection legislation;
  - Unnecessary negative impact on storage and carbon footprint;
  - Ongoing resource to manage records which no longer requires to be retained;
  - Records continue to be subject to requests under legislation.

Section 5 – Record-Specific Guidance

217 In this section you can find additional guidelines for dealing with specific record types. Further information on the record retention periods for health records and NHS corporate records can be found in Annex B.

5.1 Adopted Persons Health Records

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

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

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

221 GPs must initiate any changes of the Community Health Index (CHI) number or identity of an adopted person if it is considered appropriate to do so, following the adoption.

5.2 Adult Health Record

222 An acute/secondary care adult health record is the overarching record type for information and records collected and processed by an NHS Board about an individual aged over 16 with regards to their symptoms, assessment, diagnosis, care, and treatment. These records are created by those working within the NHS for all patient interventions across acute and secondary care. The information which would be classed as a 'adult health record' may not always be held as a single entity and may be split over formats, systems, and services.

223 This record type does **not** cover the following specialty records:

- Information held within a GP record;
- Clinical Genetics;
- Dentistry/Orthodontics/Maxillofacial;
- Mental health including; Psychiatry, Psychotherapy, Psychology;
- Learning Disability;
- Midwifery;
- Oncology;
- Ophthalmology/Orthoptics;
- Sexual Health, Genito-Urinary Medicine & Reproductive Health.

224 An adult health record may be in paper or digital format (or both) and may contain any or all of the additional record formats:

- Unstructured digital text, narrative;
- Digital forms;
- Scanned documents;
- Emails;
- Medical illustrations;
- Microfilm/microfiche;
- Photographs;
- Ultrasound scans;
- Video/voice recordings;
- X-ray films/reports.

225 It will contain some or all of the following information:

- personal data and demographics;
- diagnosed health conditions;
- treatments and prescribed medication;
- tests, procedures, operations, and results;
- allergies and past reactions to medicines;
- care plans and referrals to other services;
- lifestyle information, e.g. alcohol and nicotine intake;
- hospital admission and discharge information.

226 The record may hold information from any of the following health specialties:

- AHP Services
- Anaesthetics
- Audiology
- Cardiology
- Clinical Neuropsychology
- Clinical Health Psychology
- Dermatology
- District/Community Nursing
- Ear, Nose & Throat
- Emergency/Unscheduled Care
- Endocrinology
- Gastroenterology
- General Medicine
- General Surgery
- Geriatric Medicine
- Gynaecology
- Haematology
- Homeopathy
- Immunology
- Infectious Diseases
- Intensive Care Medicine
- Major Trauma
- Neurology
- Occupational Medicine
- Orthopaedics
- Palliative Medicine
- Plastic Surgery
- Radiology
- Rehabilitation Medicine
- Renal Medicine
- Respiratory Medicine
- Rheumatology
- Trauma & Orthopaedic
- Tropical Medicine
- Urology
- Vascular Surgery

227 Information pertaining to a person, regardless of format, should be retained in the appropriate clinical system or, where these still exist, the paper record. Emails, referrals, care plans detailing information about a person's care should be saved to the appropriate record, not within a local storage area with limited access.

228 A single retention period has been introduced for adult health records being held within digital clinical systems (that do not include the specialties listed at paragraph 200), which is to retain until three years after death. This is in order to simplify the application of retention to systems and in recognition of the interdependencies of systems across the health and social care landscape due to the integration of health and social care records.

229 Health Boards should ensure that they have appropriate processes in place to transfer deceased patient health records to their designated place of deposit. It is recommended that Health Boards sample a minimum of two generic records each year for archival preservation. This will provide the country with invaluable information on the treatment of patients throughout history. It is also recommended that Health Boards transfer records of patients who have exceptionally rare diseases/conditions or have received pioneering treatment. To support this, Health Boards should put in place a process for clinicians to identify these records, by marking a paper record or flagging/coding it on a system.

5.3 Allied Health Professional Health Records

230 Allied Health Professionals will create records during the course of their interventions with patients to deliver the following services:

- Arts therapy
- Diagnostic radiography
- Dietetics
- Occupational therapy
- Orthoptics
- Orthotics
- Paramedical Services
- Physiotherapy
- Podiatry
- Prosthetics
- Speech and language therapy
- Therapeutic radiography

231 These records require to be managed alongside the core adult/childrens record or referring specialty record e.g. mental health record. The records should be stored within the core or referring specialty record in order for them to be retained for the appropriate retention period. Where these records are not stored within other records, they should be treated as a core or referring specialty record and stored for the same retention period, with the exception of radiology images.

5.4 Ambulance Service Health Records

232 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.).

233 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).

234 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.

5.5 Asylum Seeker Health Records

235 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 digital 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, handheld records are not the standard.

236 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.

5.6 Childrens Health Record

237 A childrens health record is the overarching record type for information and records collected and processed by an NHS Board about an individual aged under 16 with regards to their symptoms, assessment, diagnosis, care, and treatment. These records are created by those working within the for all patient interventions across acute and secondary care.

238 This record type does **not** cover the following specialty records

- Information held within a GP record;
- Clinical Genetics;
- Dentistry Orthodontics/Maxillofacial;
- Mental Health/Psychiatry/Psychotherapy/Psychology;
- Learning Disability;
- Midwifery/Obstetrics;
- Oncology;
- Ophthalmology/Orthoptics;
- Sexual Health, Genito-Urinary Medicine & Reproductive Health.

239 A childrens health record may be in paper or digital format (or both) and may contain any or all of the additional record formats:

- Scanned documents;
- Emails;
- Medical illustrations;
- Microfilm/microfiche;
- Photographs;
- Ultrasound scans;
- Video/voice recordings;
- X-ray films/reports.

240 It will contain some or all of the following information:

- personal data and demographics;
- diagnosed health conditions;
- treatments and prescribed medication;
- tests, procedures, operations, and results;
- allergies and past reactions to medicines;
- care plans and referrals to other services;
- lifestyle information, e.g. alcohol and nicotine intake;
- hospital admission and discharge information.

241 The record may hold information from any of the following health specialties:

- AHP Services
- Anaesthetics
- Audiology
- Cardiology
- Dermatology
- District/Community Nursing
- Ear, Nose & Throat
- Emergency/Unscheduled Care
- Endocrinology
- Gastroenterology
- General Medicine
- General Surgery
- Gynaecology
- Haematology
- Immunology
- Infectious Diseases
- Intensive Care Medicine
- Major Trauma
- Neurology
- Neonatal
- Orthopaedics
- Palliative Medicine
- Plastic Surgery
- Radiology
- Rehabilitation Medicine
- Renal Medicine
- Respiratory Medicine
- Rheumatology
- Trauma & Orthopaedic
- Tropical Medicine
- Urology
- Vascular Surgery

242 Where there is ongoing care at the age of 16, the childrens (secondary care) record will transition into an adult record in its entirety. Where there is no ongoing care and the record does not contain information which would require to be retained for longer (see Annex B Records Retention Schedule), then the record (paper or digital) can be destroyed after the person reaches the age of 25.

243 It is recommended retaining childrens health records until the person reaches the age of 25 regardless of whether they are living or deceased. This is to enable the availability of records to assist in the treatment of siblings, particularly where there are genetic conditions and also takes into account the ongoing Scottish Child Abuse Inquiry.

244 Health Boards should ensure that they have appropriate processes in place to transfer deceased patient health records to their designated place of deposit. It is recommended that Health Boards sample two generic records each year for archival preservation. This will provide the country with invaluable information on the treatment of patients throughout history. It is also recommended that Health boards transfer records of patients who have exceptionally rare diseases/conditions or have received pioneering treatment. To support this, Health Boards should put in place a

process for clinicians to identify these records, by marking a paper record or flagging/coding it on a system.

5.6.1 Health Visitor Records

245 Health visitors will hold records for the children under their health care. Where these are held separately to the Child Health Team record, NHS Boards should have processes in place to ensure that childrens records are transferred from the Health Visiting Teams to the Child Health Teams when the child reaches school age in order that the records can be maintained together.

5.6.2 School Health Records

246 In line with all patient health records, each child should have their own school health record rather than a single record for the school or per year intake. This ensures that the information about each child is held together meaning that access is restricted to only those caring for that specific child. This also means that it can be transferred to a new school if required. This must only be done once it is confirmed the child is now resident in the new location. The record must be transferred securely. The recipient of the record should contact the sender to confirm receipt of the record (if appropriate).

247 Schools may process some health data on behalf of the NHS, in which case they must follow the records management and data protection processes set by the NHS. Irrespective of the locality of the school, it is the Health Board in which the child resides who is responsible for/the owner of these records.

248 Local Authorities are the controller for health-related information held within school records for their own purposes for example as part of Integrated Support Plans. Where the school is independent, the school itself will be the controller.

249 School Health Records processed on behalf of the NHS, stored on a school premises, must have access restricted to the NHS staff (e.g. school nurse, educational psychologist) delivering care and only be accessed by others where there is a legitimate requirement.

250 These records are subject to the retention periods in this Code of Practice regardless of where they are stored.

5.7 Clinical Psychology Records

251 Records created by Clinical Psychologists, Counselling Psychologists and Clinical Associate's in Applied Psychology during the course of treatment require to be managed alongside the core adult/childrens record or aligned specialty record.

252 The records should be stored within the core or aligned specialty record in order for them to be retained for the appropriate retention period. Where these records are not stored within other records, they should be treated as a core or aligned specialty record and stored for the following retention periods.

- Records created for patients under the care of mental health services should be held for 20 years after last seen or 3 years after death.
- Records created for patients under the care of acute psychology services, e.g. for clinical assessment prior to proceeding with bariatric surgery, are held within the core adult/childrens record.
  - Records for adults would be held for 6 years after last seen or 3 years after death, (whichever date is sooner in both scenarios for paper records and the later for digital records).
  - Records for children would be held until the child turned 25, whether living or deceased; or where there is ongoing care these would transition into the adult record.
- Records for neuropsychology care should be retained for 20 years after last seen or 3 years after death, and where neuropsychological assessment has been part of care for long term condition, retention of records should be for the duration of illness as per guidance in section 5.16.

253 Some types of test materials used by clinical psychologists require extra security and care in order to protect their integrity. They should be handled in accordance with user agreements and/or user terms and conditions. Organisations should have policy and procedure in place to ensure this is the case.

5.8 Complaints Records

254 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. The master copy of the complaint including all associated information, e.g. staff statements, should be held within the organisation's complaint handling team until it exceeds its retention period. Duplicate copies should be held by managers/those involved in investigating the complaint, for a short period of time after the complaint is closed.

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

256 The Scottish Public Service Ombudsman[30] provides complaints guidance for public authorities. Organisations may develop processes specific to their organisation which should include how complaints records should be managed e.g. the NHS Scotland Complaints Handling Procedure[31].

5.9 Controlled Drugs Regime

257 Refer to NICE 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.

[30] SPSO How to handle complaints (spso.org.uk)
[31] SPSO / Scot Gov - NHS Model Complaints Handling Procedure (spso.org.uk)

258 Further information can be found on the Healthcare Improvement Scotland (HIS) website on the safe management and use of controlled drugs.

5.10 Deceased Person's Health Record

259 Although data protection laws do not apply to data relating to the deceased, the Common Law duty of confidentiality[32], the right to respect for privacy under Article 8[33] of the Human Rights Act 1998, and the ethical obligation to respect a patient's confidentiality, extends beyond death. The duty of confidentiality and right to privacy 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;
- Medical Certificates of Cause of Death (MCCD);
- 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.

260 The FOISA (section 38(1)d) provides an exemption from the general right of access health records of a deceased person for up to 100 years from the date of the record. 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, students or minors should be maintained for 100 years from the beginning of the calendar year following the date of the last entry of the record.

261 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.

262 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.

[32] GMC Confidentiality: good practice in handling patient information - professional standards (gmc-uk.org)
[33] Human Rights Act 1998 (legislation.gov.uk)

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

264 As with the Data Protection Act 2018, a medical professional or the 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 data under Data Protection Act 2018).

265 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.

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

267 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.

268 The retention schedule 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.

5.11 Employee Records

269 Employee records contain information about a person regarding their employment within an organisation. They should hold sufficient information about an employee to track their employment history and for decisions to be made about employment matters.

270 The primary record for each employee should be held by the organisation’s Human Resources department. This record will be created during recruitment processes for new employees and should hold personal data about the employee, i.e. name, address, demographics and also recruitment records, i.e. right to work checks, contract terms and conditions, job description, next of kin details. This record will require to be kept up to date for the duration of the person’s employment, in terms of changes to home address/next of kin, contract amendments i.e. decrease in hours, change of base, recruitment to new post. This record should provide a clear employment history with regards to dates of employment, positions held and location of base.

271 It is common practice within large health care organisations for the line manager to hold the main employee record, containing information relating to the day to day management of the employee. Where this is the case this information should be managed as one record per person for the duration of their career and must be stored securely to ensure there is no inappropriate access. The main employee record will hold various different documents, including but not limited to:

- Job description and contract;
- Access forms for systems and property;
- Training records/certificates for courses attended throughout employment;
- Absence records i.e. return to work forms, maternity/paternity leave forms;
- Copies of 'Fit to Work' forms – employees should retain the original;
- Personal development or appraisal paperwork;
- Occupation health information, including any exposure to asbestos, radiation and other chemicals which may cause illness in later life;
- Work-related injury information, including applications for injury allowance scheme;
- Risk assessments e.g. Display Screen Equipment assessment;
- Records of discussions e.g. regarding poor timekeeping.

272 Where records of discussions are created and stored, this should be carried out in line with relevant workforce policies and procedures. Staff members should be aware of the record and have the opportunity to contribute or review accuracy prior to this being added to the record.

273 Some pension information may be held within either the primary or main record; however, it is likely that this information will be held within payroll records. This information should be retained until the persons 75th birthday or 6 years after the termination of contract, whichever is longer.

274 It is recommended that copies* of information relating to training courses completed by the employee should be retained within their record for their entire employment with the organisation; this is particularly important for statutory, mandatory and professional. *The employee may keep the master copy in order that they can share these with future employers if required.

275 When an employee moves to a different post within the same organisation, the main employee record must be passed to the new line manager in order to ensure the continuity of the record. The content of the record should be reviewed prior to transfer and consideration given as to whether all information within the record can be disclosed to the new manager. The primary employee record held within the Human Resources department should be updated to reflect the change in position, line manager and base.

276 When an employee leaves the organisation the main employee record should be reviewed and transferred to the Human Resources department for inclusion within the primary record. Where this is not possible it is advisable that leavers files are moved to a secure central repository overseen by the Human Resources department and/or those responsible for corporate records management, to be held until the destruction date. Organisations may wish to consider whether a sample or subset of

information about 'leavers' should be collated annually for transfer to a designated place of deposit for archival preservation.

277 Organisations should develop local guidance outlining how employee records are managed within their organisation, including what they should contain, what format they should be held in, where they should be stored, what the file structure and naming conventions should be and the security measures which must be put in place to prevent in appropriate access.

278 Within Health and Social Care partnerships, there can be instances where a line manager and employee are employed by different organisations. The main employee record maintained by or on behalf of the line manager remains under the ownership of the employee's employing organisation and should be managed in accordance with that organisation's policies (and, where the employing body is an NHS Board, in accordance with this Code of Practice). Where there are a range and variety of models currently in use, local arrangements may require to be put in place. These arrangements should be agreed in discussions with both organisations Records Managers/Data Protection Officers. The access to/sharing of employee records should be recognised in local information sharing agreements.

5.11.1 Employee Investigation Records

279 Organisations must ensure that they have adequate written processes in place for the management of employee investigation records outlining what they should contain, what format they should be held in, where they should be stored, what the file structure/naming conventions should be and the security measures which must be put in place to prevent inappropriate access.

280 The master copy of the investigation file should be managed by the Human Resources department. Copies of these files will be provided to key individuals involved in the process. The Human Resources department should clearly be able to identify what documents within the record have been provided to key individuals, when they were provided, whether they were redacted or not and why they were provided. The copies should be held by key individuals in the organisation only until the appeal period has lapsed and the investigation is fully concluded. The master copy will be retained for the retention period.

281 Where there are multiple employees under investigation for the same incident or within the same department, this can be held as one record however each piece of documentation within the record, e.g. statements, reports should only refer to one member of staff under investigation.

5.11.2 Employee Clinical/Educational Supervision Records

282 The supervisor's record should ideally be held in a centralised, access controlled system. However in the absence of such a system, at present supervisors will also require to store these records within their own 'personal drive' or 'OneDrive'. If the supervisor leaves the organisation, they must ensure that any issues/concerns are raised with the supervisee's line manager. It may be appropriate in this scenario for the supervision records to be passed to a new supervisor or to the line manager for the retention period as outlined in the retention schedule.

283 The supervisee can store their supervision records within their 'personal drive' or 'OneDrive' for as long as they feel is required. This forms part of their own personal employment record.

284 Records in relation to line management supervision should be stored by the line manager within the staff record and will be retained in line with the retention period for the staff record.

5.12 Family Health Records

285 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 (individuals' records pointing to the family record held within the lead individual record).

286 The health 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.

287 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.

288 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.).

289 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.

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

5.13 Fertility Treatment Records

291 The Human Fertilisation and Embryology Authority (HFEA) Code of Practice [34]refers to specific retention period as per Direction 0012[35].

292 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.

[34] Human Fertilisation and Embryology Authority Code of Practice (hfea.gov.uk)
[35] Human Fertilisation and Embryology Authority General Direction 0012 Retention of Records (hfea.gov.uk)

293 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.

294 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.

295 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.).

5.14 General Practitioner Records

296 GP records are the primary record of health care from birth to death. Discharge letters and correspondence from other services, e.g. secondary care, must be included in the main record. The GP record transfers with the individual as they change GP throughout their lifetime.

297 The GP record for an individual must be held for the lifetime of the patient, and ten years after death (longer periods may apply in instances of, public inquiries, investigations, fatal accident inquiries etc.).

298 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 10 years after death or 10 years after they deregister with the practice.

299 When a patient deregisters with a GP practice the following processes should be undertaken dependant on the format of the record:

- The patient's paper record should be transferred to NHS Scotland Practitioner Services who will arrange for the records to be passed to the new GP practice.
- The patient's digital record should be copied to the new practice via MedEx. The previous practice should ensure the records is passed digitally in its entirety. The previous practice should then retain their copy of records for deregistered patients for 10 years.

300 When a patient dies, NHS Scotland Practitioner Services will notify the GP Practice that the patient is registered with. The practice should retain the record for 10 years or longer where further investigations are taking place e.g. medical legal claims, investigations, public inquiries etc. Where it is felt that records should be retained for research purposes, the records should be transferred to NHS Scotland Practitioner Services who will retain records for research purposes.

301 The Primary Care Informatics Group have published a number of guidelines concerning the management of GP patient health records; Guidance – Primary Care Informatics (scot.nhs.uk).

302 Also see section 3.0 Responsibilities of processors and sub-contractors.

5.15 Integrated Care Records

303 Integrated or joint care records held by health and social care organisations are subject to local governance arrangements. The partner agencies involved must consider and agree controller/processor roles, scope and purpose of the records, retention schedules, security measures, and work instructions for accessing or updating the records etc. The integrated records agreement must identify the legal basis for the processing across the Partnership, including any data sharing with additional partner agencies.

304 Currently there is no prescribed approach, each public body is responsible for maintaining compliance with all relevant legislation, including the regulatory framework outlined in section 2.3.

305 Potential usage of integrated records includes:

- online portals with role-based access permissions that can be used by several agencies to access the same record/information for different purposes;
- Anticipatory Care Plans or Integrated Care Records;
- fully integrated Customer Relationship Management (CRM) systems.

306 Regardless of the approach taken for integrating health and social care records, an integrated records agreement should be in place and records management rules must be mutually agreed.

307 The NHSS Information Sharing Toolkit should be used wherever NHSS data is concerned.

308 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 Condition (LTC) Health Records

309 Long Term Conditions records are necessary for continuity of health care. A long term condition is a condition which cannot at present be cured but can be controlled by medication and therapies.

310 Long term conditions include, but are not limited to:

- Angina
- Arthritis
- Asthma
- Atrial Fibrillation
- Back Problems
- Chronic Obstructive Pulmonary Disease
- Coronary heart disease
- Depression
- Diabetes
- Epilepsy
- Heart Failure
- Hepatitis
- Hypertension
- Inflammatory Bowel Disease
- Kidney failure
- Multiple sclerosis

311 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. Where the secondary health care record requires to be retained, Health Boards should consider putting processes in place to identify records for long term conditions through coding or flagging/marking digital and paper records to ensure that they are identifiable.

312 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 MAPPA Records

313 Multi-Agency Public Protection Arrangements (MAPPA) records are created to support the arrangements in association with managing the risks of serious harm to the public. The Responsible Authorities involved in these arrangements are Police Scotland, Local Authorities, NHS Boards and Scottish Prison Service.

314 As per 5.12 of the National Guidance[36], the MAPPA Co-ordinator for the relevant Local Authority is the Single Point of Contact (SPoC) for all notifications (and referrals). The MAPPA Co-ordinator should maintain an accurate record of the number of individuals being managed by the Responsible Authorities in their area. Where copies of documents relating to individuals managed under MAPPA are required which are not readily available on Health systems, a request should be made to the local MAPPA Co-ordinator or MAPPA Health Liaison Officer.

315 Within Health Boards, MAPPA records are held separately from the patient's health records, however alerts may be placed on patient health records in relation to MAPPA arrangements. Copies of records shared by the MAPPA Coordinator with Health Boards, should be stored securely in accordance with their security classification and retained for a minimum amount of time. Health boards (with the exception of the State Hospital), require to retain master copies of records pertaining to the notification to add/remove an alert to a patient record and minutes of internal NHS MAPPA meetings.

316 Where the State Hospital is the Lead Authority for a MAPPA case, generally a restricted patient, they will require to hold the master copy of MAPPA records (notifications, referrals, risk management plan, case review meeting minutes). These records should be held in line with the retention periods within the National Guidance which states: The nominal record will be retained until the 100th anniversary of the individual's birth.

[36] Scottish Government Multi-Agency Public Protection Arrangements National Guidance (gov.scot)

5.18 Maternity Records

317 Maternity records relating to the health care of a mother and baby during pregnancy, labour and the puerperium must be retained to support the health care to be given to the woman during her reproductive life, and/or her baby, and any future children. Local procedures should be in place which clearly specify particular records to be retained AND include detail regarding transfer of records and needs for the final collation of the records for storage (where paper records still exist); for example, the necessity for inclusion of community midwifery records. The procedure should also determine details of the mechanisms for the return, collation, and storage of those records, which are held by mothers themselves, during pregnancy and the puerperium.

318 Maternity Records should include the following:

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

319 Health Boards require to retain obstetric/maternity records until 25 years after the end of the last pregnancy or until the woman reaches the age of 50 due to there being a greater occurrence of women giving birth at more spaced periods of time until later in life. It is also recognised that maternity records can support the health care of siblings especially where genetic conditions were identified.

5.19 Medical Court Reports

320 As part of their professional role, clinicians can be requested to provide a report for Court regarding an individual who is going through the criminal justice process. Clinicians may be asked to do this as part of their NHS employed role or under a private agreement.

321 Court reports should not be stored within the patient's health record. Equally the reports do not require to be stored as part of the organisation's corporate records as the organisation has no justifiable purpose for retaining the information. However, it is recognised that clinicians may wish to store a copy of these reports following the submission to court, for their own reference purposes, should they be called to court regarding their report. Given the sensitivity of the reports it is appropriate for these reports to be stored on the clinician's employer's digital network in order that they are stored securely.

322 It is advised that the clinician's own copies of the reports which they have submitted to court should only be retained for the period that the clinician is liable to require to reference the report. Where a clinician changes employer, they should ensure that any court reports which they continue to require access to are moved to a personal repository or their new employer. Any court reports which are no longer required due to completion/closure of the court case should be destroyed confidentially.

323 There is no obligation on NHS Boards to retain copies of court reports. Courts hold the master version of the report for 25 years following which it is passed to the National Records Scotland for permanent preservation.

5.20 Medical Device Records

324 During the course of the delivery of health care, medical devices can be used to support assessment, diagnosis, monitoring and treatment. This could be hardware, software, or appliances ranging from sticking plasters to catheters to pace makers.

325 Where a medical device has been implanted in a patient as part of the care, which is not removed prior to discharge from a hospital or care setting, Health Boards must ensure that records regarding the implantation of the device are retained for the lifetime of the patient plus three years after death even if the device is removed. Examples of implantable medical devices which may not be removed prior to discharge from a hospital or care setting include but are not limited to joint replacements (hip/knee), metal pins, pacemakers, intrauterine device, corneal rings.

326 The legislation covering medical devices is the Medicines and Medical Devices Act 2021[37] and the UK regulation of medical devices is managed by the Medicines and Healthcare products Regulatory Agency (MHRA).

5.21 Meeting Records

327 Meeting records should generally be recognised as vital corporate records. They can form part of the organisation's corporate memory, providing evidence of discussions which have taken place at meetings, the outcomes, decisions and actions required in order to support its daily function and operations. They can also provide crucial information which may be used as evidence for investigatory purposes or can be requested under legislation. Meeting records include the agenda, associated papers and minute of the meeting.

328 Meeting records are usually produced for established groups or committees as part of an accountability framework where the purpose is to achieve a stated objective and follow a clear meeting agenda. However, records can also be required for unplanned emergency meetings and investigatory meetings. At meetings where the outcome of the discussion requires to be recorded, minutes of the meeting should be produced in the form of a formal written (typed) minute. It is recognised that audio-visual recording and transcription technology is evolving; however, this technology should not be used in place of the production of a formal written (typed) minutes for meetings where these records are required.

[37] Medicines and Medical Devices Act 2021 (legislation.gov.uk)

329 Minutes of meetings are a record that the meeting occurred, and outline the topics discussed/actions agreed in meetings. They allow for actions to be tracked, people to be held accountable for actions, those not present to be fully appraised of all discussion and assist in decision making. They can be used as evidence for legal purposes to prove decisions and actions. Minutes of meetings can be of historical importance as they record how the organisation functioned and made decisions in the past. As the organisation evolves, the minutes of meetings from the past can be used as a reference to show how topics were handled and why. Therefore robust processes should be put in place to manage this record set appropriately.

5.22 Mental Health Records

330 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 or where a patient in under the care of mental health services within an NHS Board.

331 Records for any person who in under the care of mental health services or has been detained 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 or 3 years after death if sooner. 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.

332 Records which relate to the detention of a person under the Mental Health (Care & Treatment) (Scotland) Act 2003 require to be completed by the treating NHS Board. Copies of the documentation require to be provided to the Mental Welfare Commission at the time of detention and on revoking the detention to afford the Mental Welfare Commissioner all facilities necessary for them to discharge their functions under the Act, as per Section 17 of the Mental Health (Care and Treatment) (Scotland) Act 2003. These records are not stored within the person's main mental health record and there is no ongoing obligation for the treating NHS Board to retain this documentation. Records in relation to the detention of a person under the act, once provided to the mental Welfare Commission should be retained to the end of the year which they relate to plus one year, after which they can be destroyed.

333 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).

334 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 serious incidents or genetic implications of the patient's illness. If it is decided to retain the records, they should be subject to regular review.

335 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.

5.23 NHS 24 Records

336 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.

5.24 Occupational Health Records

337 The main occupational health record must be kept separate from the main employee record and classified as a health record (whereas the employee record is classified as a corporate record). The occupational health record may contain information regarding an employee's physical and mental health symptoms, diagnosis, ongoing treatment being received, information related to any injuries sustained within the workplace, vaccinations, health surveillance questionnaires, radiation exposure and proposed support, onwards referrals and reasonable adjustments which are recommended.

338 Occupational health information requires to be shared with a Line Manager in order for them to support employees, particularly in terms of making reasonable adjustments under the Equality Act 2010. Consent will be sought from the employee prior to sharing this information. Where information/correspondence is provided to a Line Manager from the Occupational Health department it must be stored within the employee record for the duration of the employee's career within the organisation.

339 When occupational health records are outsourced, the controller must ensure the processor/contractor can retain the records for the duration of the contract between the controller/processor and that there is a process for the records to be returned back to the organisation upon termination of the controller/processor contract. A process should also be put in place to notify the processor of leavers from the controller organisation in order that this can trigger the six-year retention for the records of those employees who have terminated their employment.

5.25 Oncology Records

340 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.

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

342 The Royal College of Radiologists state 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 health 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.

343 Wherever possible, oncology records should be in a preserved digital format.

344 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.

345 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.

5.26 Patient/Client-Held Health Records

346 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.

347 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 controller and include a return address if they are lost.

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

349 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.

5.27 Prison, Youth Offenders & Secure Units (Mental) Health Records

350 **Prison Health Records.** 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.

351 **Youth Offending Service Health 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 birthday unless other criteria apply (e.g. mental health, Child Abuse Inquiries, appraisal for permanent retention etc.).

352 **Secure Unit Mental Health Records.** Some institutions that care for offenders are categorised as hospitals because the offender is considered a patient and has been detained under the Mental Health (Care and Treatment) (Scotland) Act 2003. 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.

5.28 Public Health Scotland Records

353 Public Health Scotland is the National Statistics provider for health and social care in Scotland. As part of its remit to support the improvement of the health and wellbeing of the population of Scotland and address the public health challenges, it engages in processing activities which include:

- Collecting/receiving defined data;
- Analysing data and producing health intelligence which inform the actions necessary to address public health challenges in Scotland;
- Supporting research and curating safe data for controlled and authorised access via the national safe haven;
- Evaluating long term impact of national and local policies;
- Publishing long term anonymised trend information.

354 The organisation processes this data in the public interest and as per its legal obligation under the following laws and regulations:

- Statistics and Registration Service Act 2007;
- Official Statistics (Scotland) Amendment Order 2019;
- Code of Practice for Statistics 2022;
- Public Health Scotland Order 2019;
- Public Health etc. (Scotland) Act 2008;
- National Health Service (Scotland) Act 1978;
- International Health Regulations (2005);
- UK Focal Point Communications Protocol on Serious Cross-border Threats to Health.

355 Public Health Scotland will retain personal data for as long as processing is necessary in the public interest to meet its obligations as the national public health agency for Scotland. These retention periods will be detailed and justified in Public Health Scotland's relevant data protection impact assessments which support the processing and set out its local records management retention policy.

356 Public Health Scotland will impose retention periods on personal data which is no longer necessary for processing. Examples include when a bespoke analytical project runs for a defined period and comes to an end, when the outputs are published as part of its transparency obligations in compliance with the code of practice for statistics. The retention periods will be specified in the relevant data protection impact assessments.

5.29 Public Inquiry Records

357 In the event of an Inquiry being convened under the Inquiries Act 2005 (see section 2.3.5), organisations should take action to ensure it is able to capture and retain records as evidence. Records identified as being of potential relevance to the inquiry must not be destroyed or disposed of until there is clear instruction from the inquiry team that they are not required.

358 It is recommended that the following steps are undertaken:

- Issue a communication to raise awareness of the Inquiry and requirement to identify and protect information and records which may be of relevance;
- Amend retention schedules/records management policies to highlight the requirement to protect relevant documentation from destruction;
- Undertake a scoping exercise to identify the information and records of relevance, where they are stored and the volume;
- Agree a single point of contact for the collation of evidence;
- Agree how and where evidence will be stored once collected;
- Ensure that an accurate inventory of records submitted is held by the organisation and maintained. In some instances, the Inquiry Team will also expect an inventory to accompany each submission of evidence/statements.

359 Information or records, in the form of statements or evidence, submitted to the Inquiry must be retained as part of the Inquiry record permanently and when appropriate deposited with the designated permanent place of deposit.

360 Records which were retained beyond their retention period due to the inquiry, however, were then deemed not relevant or not used in the proceedings of the inquiry can be destroyed one year after the closure of the inquiry.

5.30 Sexual Health Records

361 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 infections 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.

5.31 Sexual Offence Examination Records

362 The Forensic Medical Services (Victims of Sexual Offences) (Scotland) Act 2021 (FMS Act) places a statutory duty on health boards to provide Forensic Medical Examination (FME) and healthcare services for victims of sexual offences. Each health board has established a Sexual Assault Response Co-ordination Service (SARCS). A person can access a SARCS if they report the incident to the police within the 'forensic window' (seven days), or they can self-refer without first having to make a report to the police. Information on the service can be found on the NHS website.

363 The Forensic Medical Services (Self-Referral Evidence Retention Period) (Scotland) Regulations 2022 sets out specific retention periods for the evidence gathered during a FME which can be found detailed within the retention schedule.

364 Section 17 of the FMS Act clarifies that “evidence” does not include information that is gathered for a purpose other than to be used for a police investigation or subsequent proceedings: for example, information gathered for the purpose of determining a person’s healthcare needs following the incident is not considered evidence. Records relating to healthcare information gathered at the same time as the forensic medical examination, for example the healthcare form and associated healthcare records, should be stored, retained and destroyed in line with adult health record retention periods.

365 Section 9 of the FMS Act sets out the situation where the offence is reported to the police. The appointed police officer will contact the SARCS directly to arrange the uplift of evidence, statements and forensic reports and will provide a signed copy of the mandate for forensic documentation to the SARCS facility, which will then be stored with the health record. The time frame for the Health Board to retain a copy of the Sexual Offences Against Adults Forensic Form is five years from the date the forensic form is provided to the police (or when a self-referral converts to a police referral). This will ensure that clinicians are able to prepare fully for giving evidence in court without needing to request a copy of the forensic form from the COPFS. This time frame does not impact the 26-month retention period for self-referral evidence when no police report is made.

366 Section 8 of the FMS Act sets out the rules for the destruction of evidence and associated forensic information. When the record has exceeded its retention period, all documentation in relation to the forensic examination (not the health care assessment), including photographs and colposcopy images, should be securely disposed of within at least five working days of the end of the retention period, to ensure consistency in practice across the country.

367 If a person decides that following the examination they will not, at any time, be reporting to the police, they can request the health board destroy any evidence provided by them at any time before the end of the retention period. A 30-day cooling off period will apply to this request and health boards must therefore ensure that evidence is destroyed only after the expiry of the 30-day period. The exception is if the request is made in the last 30 days of the retention period, in which case any evidence must be destroyed as soon as is reasonably practicable after the expiry of the retention period (unless the person decides to report the matter to the police before the expiry of the retention period).

368 Processes must be put in place by health boards to ensure that all records associated with the evidence are retained/destroyed in line with these retention periods. A Self-Referral National Protocol has been put in place to support these processes.

5.32 Specimens and Samples

369 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.

370 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 health 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.

371 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.

5.33 Transgender Persons Health Records

372 The Data Collection and Publication Guidance, Sex, Gender Identity and Trans Status[38], provides the following definitions of sex and gender:

- **Biological sex**: as determined by a person's anatomy, which is produced by a combination of their chromosomal, hormonal, genital and gonadal characteristics, and their interactions.
- **Legal sex**: typically legal sex is their sex registered at birth. However, for a person with a full Gender Recognition Certificate, their legal sex is their acquired sex.
- **Self-defined sex**: a person's innate sense of whether they are female or male
- **Gender**: a social construction relating to a set of norms, roles and relationships that is founded in social mores, laws, processes and policies based on labels of masculinity and femininity. Gender is time- and culture-specific.
- **Gender identity**: a personal, internal perception of oneself, and so the gender category someone identifies with may not match their sex registered at birth. What an individual experiences as their innate sense of themselves as a man, a woman, as having no gender identity, or as having a non-binary gender, where people identify as somewhere on a spectrum between man and woman
- **Transgender:** anyone whose gender identity differs from their sex registered at birth.

373 Transgender patients have rights in having their gender identity recognised and recorded in their health records. However, cognisance needs to be taken that this may have unintended negative consequence to their overall health, where a name and gender identity is recorded which differs from their biological sex at birth, and

[38] Sex, gender identity, trans status - data collection and publication: guidance (gov.scot)

new health records are not appropriately linked to previous records.[39]

374 Within a health and social care setting, patients have the right to request to change their Male/Female marker on their patient health record without the requirement of a Gender Recognition Certificate (GRC) or updated birth certificate. Patients can choose to be issued with a new CHI number to reflect their gender identity. Once the patient has been issued with a new CHI number, a new record is created which is linked to the patient's previous record, known as the 'historic' record. Male/Female markers and any demographic information related to the patient's previous identity should be removed from the historic record. Information related to previous healthcare provided which would indicate that the person has changed gender, for example reference to a breast or genital examination, should remain. Information on the requirements for processing a change of record can be accessed via NHS National Services Scotland - How to change patient details (nss.nhs.scot).

375 The Gender Recognition Act 2004[40] allows individuals to change their legal sex by obtaining a GRC which allows an updated birth certificate to be issued showing their updated legal sex. A patient who does not obtain a GRC retains the legal sex as identified on their birth certificate. However, whether or not they have a GRC, transgender patients have a range of rights on the basis of their gender reassignment under section 7 of the Equality Act 2010[41] which provides "A person has the protected characteristic of gender reassignment if the person is proposing to undergo, is undergoing or has undergone a process (or part of a process) for the purpose of reassigning the persons' sex by changing physiological or other attributes of sex." The Equality Act 2010 does not require a patient to be under medical supervision to have this "protected" characteristic.

376 Under section 22 of the Gender Recognition Act 2004 (Gender Recognition Act 2004 (legislation.gov.uk)) it is a criminal offence for "a person who has acquired protected information in an official capacity to disclose the information to any other person". Protected information refers to either a person's application for, **or** their gender identity prior to obtaining, a Gender Recognition Certificate to change their legal sex. There are various exceptions specified in section 22 and in Orders under the section[42] which allow for some protected information to be disclosed.

377 When documenting a patient's gender identity, it is important that their human rights, legal rights and rights to privacy are considered. In some circumstances during the provision of health care, it will be important for clinicians to have access to both biological sex and gender identity to support the appropriate provision of care and treatment, whilst upholding the patient's rights. Decisions based on, for example test results, can differ between those with chromosome XX and those with chromosome XY due to physiological and biological differences. Therefore a clinical risk could be created if the biological sex is not known and/or accessible via a historic record, as a treatment pathway may be required to be based on the patient's biological sex

[39] Electronic medical records and the transgender patient: recommendations from the World Professional Association for Transgender Health EMR Working Group (nih.gov)
[40] Gender Recognition Act 2004 (legislation.gov.uk)
[41] Equality Act 2010 (legislation.gov.uk)
[42] The Gender Recognition (Disclosure of Information) (Scotland) Order 2005 (legislation.gov.uk) and The Gender Recognition (Disclosure of Information) (Scotland) Order 2023 (legislation.gov.uk)

instead of their gender identity. This consideration should be discussed with patients who are requesting to amend their health record, most commonly the CHI number.

378 Initiatives are underway across health care to review systems and consider how they can be adapted to collect both biological sex and gender identity. When undertaking this work, groups should be mindful of the information and further guidance which is contained within this section.

379 Further advice can be found on the following links:

- MDDUS - The care of transgender patients by GPs (mddus.com)
- GMC Ethical Hub - Trans healthcare (gmc-uk.org)
- Sex, gender identity, trans status - data collection and publication: guidance (gov.scot)

5.34 Witness Protection Health Records

380 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.

381 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.

5.35 Records in Specific Formats

5.35.1 Medical Images and Video Recordings

382 During the course of health care, patients will undergo tests and procedures to support the diagnosis and treatment of their symptoms and conditions. At times this may involve procedures which result in the production of images or recordings. Images and recordings will be reviewed by the appropriate clinical staff and in some cases a report will be produced detailing the outcome of the review of the image/recording and the professional opinion of the clinician with regards to the findings, diagnosis, treatment and/or further procedures required.

383 It is acknowledged that the file size of medical images and medical recordings may in some cases be significant and the long term storage of these will have an impact on storage capacity and costs associated with this. Where a summary/outcome report has been created there may not be a requirement for the image/recording to be retained for the lifetime of the patient and a further three years after death (or up to the age of 25 if the patient died before they were 17) as the image/recording may then be able to be viewed as transitory. However, when considering the appropriate retention period for large media files used in the course of health care, advice should be sought from the organisation's Health Records Manager to ensure decisions are made on a specialty by specialty basis taking into account future care needs, retention periods of the associated specialty record, quality control processes and potential for future investigations.

5.35.2 Emails

384 Email is a format of information and not all emails will constitute a record. Organisations must have an email policy with clear rules for managing, storing, deleting, and sending/disclosing emails. Failure to manage emails indicates a weakness in records management. Organisations should consider the implementation of special training plans and an audit of working practice to identify and address poor practice. Refer to The National Archives guidance on emails for further details on the management of emails as records and the means of ensuring they are captured, managed and stored in the appropriate area so that they are accessible and usable to all relevant parts of the organisation.

385 When emails need to be retained, they must be preserved in their entirety, including any attachments, to protect their integrity. They should be saved to the correct records repository, which will not normally be the email account. Email accounts are not recognised as storage repositories for organisational records.

386 Deliberate deletion of emails (or any other information) with the intention of frustrating a request for information 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) may be a criminal office. Emails also need to be managed securely and in line with relevant policy and guidance, for example: UK Government Secure email guidance (gov.uk).

387 Deliberate deletion of emails (or any other information) with the intention of frustrating a request for information under the Freedom of Information (Scotland) Act 2002 or a subject access request may be a criminal offence under FOISA or the Data Protection Act 2018.

388 Where email accounts are portable across organisations, processes must be put in place to ensure data is not transferred to the new organisation unless necessary. It is poor practice to purge email accounts when individuals transfer to other organisations, as some emails may be considered as corporate records, and must be kept where necessary.

389 Emails, as with all correspondence, in relation to patient health and social care, must be kept within their corresponding health and/or social care record.

5.35.3 Websites and Intranet

390 Websites and intranets are digital means to provide vital information and communications to the public and employees, in an organised manner. As published information, it is important that website and intranet content is captured and retained as part of an organisation's records and therefore they are subject to this Code of Practice. Information published on an organisation's website may influence the behaviour of an individual, who may respond to the content accordingly. It is important to capture what information was available from the site at a given moment in time and variations (updates) to content published on 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.

391 The websites of Scottish public authorities who transfer their records to the National Records of Scotland (NRS) for permanent preservation, will have their websites regularly 'snapshot' by the NRS Web Continuity Service and added to the NRS Web Archive as part of their deposit arrangements.

392 The National Library of Scotland (NLS) is entitled under the terms of the Legal Deposit Libraries Act 2003 to request a copy of all printed items published in the United Kingdom. From 6th April 2013, the Legal Deposit Libraries (Non-Print) Regulations 2013 extended this to include the right to harvest UK electronic publications, including websites. The NLS has a Memorandum of Understanding with the Scottish Government to preserve and make accessible, Scottish Government websites. This includes websites with a UK domain, e.g. .scot, or .uk. This does not cover intranets, email, databases, and anything stored in the cloud or social media. This content is archived by the UK Web Archive. Some UK Web Archive website content can be accessed via the UK Web Archive (webarchive.org.uk) website but secure access to most legal deposit copies is available only from the NLS reading rooms in Edinburgh and Glasgow.

393 In exceptional circumstances, public authorities may request the UK Web Archive to undertake web crawls and capture on their behalf. An organisation's designated place of deposit may also be able to crawl and capture website content.

394 As Intranets are utilised for communicating information internally to organisations and sit behind private IP addresses, the UK Web Archive and the NRS Web Continuity Service do not include intranets as part of their web crawl service. It is therefore the responsibility of the organisation to ensure that intranet content, or even the entire intranet, is subject to the records management process.

395 Organisations should note that a web archive does not negate the need to also transfer the original records selected for permanent preservation to a designated place of deposit, regardless of whether they are also published on websites.

5.35.4 Social Media

396 When organisations implement social media channels as a means of communication, they should put an acceptable use policy in place which also outlines the requirement for a risk assessment, process for the registration of the information asset, designation of an IAO and the requirement to follow data protection policies.

397 In a health and social care setting, social media is used for circulating information regarding the activities of the organisation or providing generic advice to the population, rather than as a way of communicating with patients about their direct care. Information posted on social media (such as health campaigns, advice on where to seek support) will usually be captured elsewhere in an organisation's corporate records function, and where this is the case, there is no value in retaining the information held in the social media platform, as it will be a duplication. However in instances where it is not captured, appropriate measure should be put in place to retain the information in line with the organisation's retention schedule. If a social

media platform is utilised by the organisation and it is possible to export posts, the schedule and analytics when required this should be done on a regular basis. Where this is not possible organisations should document the activity through transcription or periodic storage e.g. snapshot. This is especially pertinent to social media posts which could be required as part of an investigation/public inquiry or designated as of historical interest for example the coverage of a major incident such as the Covid-19 pandemic.

Annex A: Further Guidance

Further information on legal and professional obligations is available on the following websites:

- Scottish Government Information Governance

Regulatory Bodies:

- National Records of Scotland
- Information Commissioner's Office
- Scottish Information Commissioner's Office
- Care Inspectorate
- General Chiropractic Council
- General Dental Council
- General Medical Council
- General Optical Council
- General Osteopathic Council
- General Pharmaceutical Council
- Health and Care Professions Council
- Healthcare Improvement Scotland
- Nursing and Midwifery Council
- Scottish Social Services Council

Legislation:

- Access to Health Records Act 1990
- Data Protection Act 2018
- Environmental Information (Scotland) Regulations 2004
- Freedom of Information (Scotland) Act 2002
- Inquiries Act 2005
- Network and Information System Regulations 2018
- Public Records (Scotland) Act 2011
- Scottish Public Sector Cyber Resilience Framework
- UK General Data Protection Regulations

Professional Bodies - Health Sector:

- British Medical Association
- College of Dentistry
- NHS Scotland Primary Care Informatics
- Royal College of General Practitioners
- Royal College of Midwives
- Royal College of Nursing
- Royal College of Obstetricians & Gynaecologists
- Royal College of Pathologists
- Royal College of Physicians
- Royal College of Physicians and Surgeons of Glasgow
- Royal College of Surgeons of Edinburgh
- Royal Pharmaceutical Society
- UK Caldicott Guardian Council

Professional Bodies – Social Work Sector:

- British Association of Social Workers
- Coalition of Care and Support Providers in Scotland
- Scottish Association of Social Work
- Social Work Scotland

Professional Bodies – Records Management Sector:

- Archives and Records Association
- Federation for Informatics Professionals
- Information and Records Management Society
- Professional Records Standards Body
- Scottish Council on Archives
- The Institute of Health Records and Information Management

International and British Standards:

- ISO8601 - Date and Time Format
- ISO13008 - Digital records conversion and migration process
- ISO15489 - Records management
- ISO16175 - Processes and functional requirements for software for managing records
- ISO17068 - Trusted third party repository for digital records
- ISO18128 - Risk assessment for records processes and systems
- ISO21965 - Records management in enterprise architecture
- ISO23081 - Metadata for records
- ISO22428 - Managing records in cloud computing environments
- ISO26122 - Work process analysis for records
- ISO30301 - Management systems for records - Requirements
- ISO30302 - Management systems for records - Guidelines for implementation
- BS10008 - Evidential weight and legal admissibility of electronic information
- BS10010 - Information classification, marking and handling
- BS10025 - Management of Records. Code of Practice
- BS15713 - Secure Destruction of Confidential Material
- ISO/IEC 27000 - Information security overview and vocabulary
- ISO/IEC 27001 - Information security management system requirements
- ISO/IEC 27002 - Code of Practice for Information Security controls
- ISO/IEC 27017 - Information security controls for cloud services
- ISO/IEC 27031 - Information security controls on business continuity

Annex B: Record Retention Schedule

For NHS Boards and organisations contracted to work and/or managing records on their behalf, the records retention schedule can be accessed via this link:

Resources - Digital Healthcare Scotland (digihealthcare.scot)

For Local Authorities and organisations working on their behalf to deliver social care services, the baseline retention schedule can be accessed via this link:

Scottish Council on Archives Record Retention Schedules (SCARRS) (scottisharchives.org.uk)

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at

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

ISBN: 978-1-83601-544-4 (web only)

Published by The Scottish Government, August 2024

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS1479718 (08/24)