SCOTTISH GOVERNMENT

RECORDS MANAGEMENT:

NHS CODE OF PRACTICE

(SCOTLAND)

Version 1.0

June 2008

SECTION 1 – FOREWORD

Background

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

2. The guidance was drafted in collaboration with a working group made up of representatives from the Scottish Government Health Directorate, Scottish NHS archivists, NHS Health Records Managers, patient groups and GP Practices. As part of its work, the working group commissioned a public consultation on the retention and disposal of health records in 2005. The results of that consultation have informed the drafting of this guidance. The draft was updated and issued for consultation during Autumn 2007. Further information can be found **here**.

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

Aims

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

    - establish, as part of the wider information governance framework, records management best practice in relation to the creation, use, storage, management and disposal of NHS records;

    - provide information on the general legal obligations that apply to NHS records;

    - set out recommendations for best practice to assist in fulfilling these obligations, for example adhering to National Information Governance Standards;

    - explain the requirement to select records for permanent preservation;

    - set out recommended minimum periods for retention of NHS personal health records regardless of the media on which they are held, and;

    - indicate where further information on records management may be found;

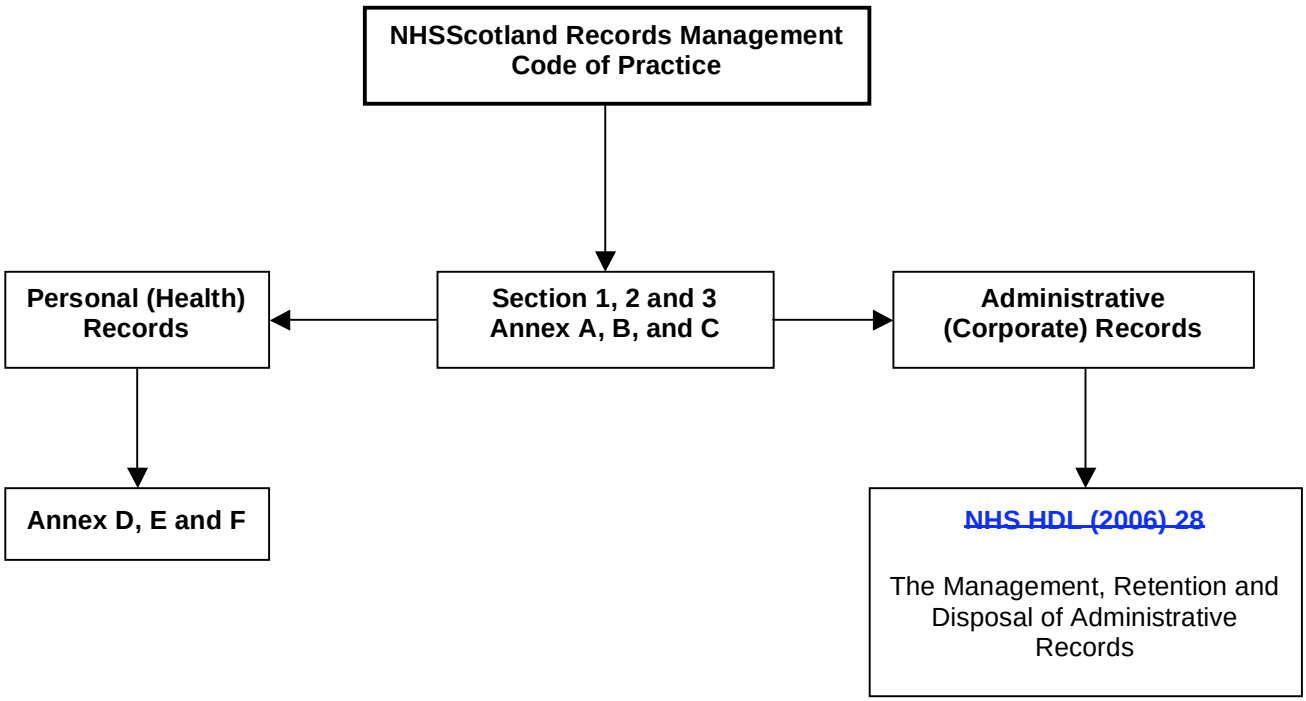
Types of Record covered by the Code of Practice

5. The guidelines contained in **Section 1, 2 and 3 and Annex A, B and C** of this Code of Practice apply to **NHS records of all types** (including records of NHS patients treated on behalf of the NHS in the private health sector) regardless of the media on which they are held:

    - personal health records (electronic or paper based; including those concerning all specialties, and GP medical records);
    - records of private patients seen on NHS premises;
    - records of blood and tissue donors;
    - accident & Emergency, birth, and all other registers;
    - theatre registers & minor operations (and other related) registers;
    - x-ray and imaging reports, output and images;
    - photographs, slides, and other images;
    - microform (i.e. fiche / film);
    - audio and video tapes, cassettes, CD-ROM etc;
    - e-mails;
    - computerised records;
    - scanned records;
    - text messages (both out-going from the NHS and in-coming responses from the patient);

Annex D, E and F apply to **Personal Health Records only**.

This is illustrated in the diagram on the below:



Please note:

- **sections 1, 2, 3 and annex D** are for implementation;
- **annexes A, B and C** are to aid understanding and provide reference to other useful information;
- **annex E and F** were produced by a sub-group of the Health Records Forum and are included as guidance on best practice to Health Boards on the development of local health record strategy and policies.

SECTION 2 – INTRODUCTION

6. This Code of Practice replaces previous guidance as listed below:

    - SHM 58/60 – Scottish Hospital Service Destruction of Hospital Records;
    - ECS(A) 21/1969 – Disposal of Records That Have Lost Their Value;
    - MEL (1993) 152 – Guidance for the Retention and Destruction of Health Records;

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

8. This is an overarching Code of Practice on records management for Scottish NHS organisations and incorporates references and links to previously published guidance, such as NHS HDL (2006) 28 Management, Retention and Disposal of Administrative Records.

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

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

    - information Governance Standards, which can be viewed on the Specialist e-Library **here**
    - information Governance Toolkit
    - NHS Scotland Information Governance Team and policy advisers in the Scottish Government eHealth Directorate.

    Further information on the above can be found in **Annex B**.

General Context

11. All NHS organisations are public authorities under Schedule 1 of the Freedom of Information (Scotland) Act 2002, and the records they create are subject to the Public Records (Scotland) Act 1937 (as amended). Scottish Ministers and all NHS organisations are obliged under Data Protection and Freedom of Information legislation to make arrangements for the safe keeping and eventual disposal of all types of their records. This is carried out under the overall guidance and supervision of the Keeper of the Records of Scotland who is answerable to the Scottish Parliament. Whilst this Code of Practice is based on the Scottish Government's understanding of the relevant law in Scotland as at the date of publication, it is not, and should not be read as,

a statement of the definitive legal position on any matter. NHS organisations should consult their own legal advisors for advice on any legal issues, which arise regarding the matters covered in this Code of Practice.

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

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

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

    Further information can be obtained **here**.

14. Chief Executives and senior managers of all NHS organisations are personally accountable for records management within their organisation. NHS organisations are also required to take positive ownership of, and responsibility for, the records legacy of predecessor organisations and/or obsolete services.

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

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

    - support patient care and continuity of care;
    - support day to day business which underpins the delivery of care;
    - support evidence based clinical practice;
    - support sound administrative and managerial decision making, as part of the knowledge base for NHS services;
    - meet legal requirements, including requests from patients or other individuals under subject access legislation or Freedom of Information;

- assist clinical and other audits;

- support improvements in clinical effectiveness through research and also support archival functions by taking account of the historical importance of material and the needs of future research;

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

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

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

Legal and Professional Obligations

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

19. Another key statutory requirement for compliance with records management principles is the Data Protection Act 1998. It provides a broad framework of general standards that have to be met and considered in conjunction with other legal obligations. The Act regulates the processing of personal data, held manually and on computer. It applies to personal information generally, not just to health records, therefore the same principles apply to records of employees held by employers, e.g. in finance, personnel and occupational health departments.

20. Personal data is defined as data relating to a living individual that enables him/her to be identified either from that data alone or from that data in conjunction with other information in the data controller's possession. It therefore includes such items of information as name, address, age, race, religion, gender and physical, mental or sexual health.

21. Processing includes everything done with that information, i.e. holding, obtaining, recording, using, disclosure and sharing of it. Using includes disposal, i.e. transfer to an archive or destruction of the record. More information on the application of the Data Protection Act is contained in Annex C.

22. Other legislation relating to personal and corporate information and the records management function generally can also be found in Annex C. Additionally, clinicians are under a duty to meet records management standards set by their governing regulatory bodies.

NHSScotland eHealth Strategy

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

Social Care Records

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

SECTION 3 – NHS RECORDS MANAGEMENT

Management and Organisational Responsibility

25. The records management function should be recognised as a specific corporate responsibility within every NHS organisation. It should provide a managerial focus for records of all types in all formats, including electronic records, throughout their life cycle, from planning and creation through to ultimate disposal. It should have clearly defined responsibilities and objectives, and necessary resources to achieve them.

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

27. The manager, or managers, responsible for the records management function should be directly accountable to, or work in close association with the manager or managers responsible for Freedom of Information, Data Protection and other information governance issues.

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

Policy and Strategy

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

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

31. The policy should also:

    - outline the role of records management within the organisation, and its relationship to the organisation's overall strategy;

    - define roles and responsibilities within the organisation including the responsibility of individuals to document their actions and decisions in the organisation's records, and to dispose of records appropriately when they are no longer required;

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

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

32. The policy statement should be reviewed at regular intervals (at least once every 2 years) and, if appropriate, it should be amended to maintain its currency and relevance.

Record Creation

33. Each operational unit (e.g. Finance, Estates, IT, Direct patient care) of an NHS organisation should have in place a process for documenting its activities. This process should take into account the legislative and regulatory environment in which the unit operates.

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

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

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

Information Quality Assurance

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

    - what they are recording and how it should be recorded;

    - why they are recording it;

    - how to validate information with the patient or carers or against other records – so staff are recording the correct data;

    - how to identify and correct errors – so that staff know how to correct errors and how to report errors if they find them; and

- the use of information – so staff understand what the records are used for (and therefore why accuracy is so important);

- how to update information and add in information from other sources.

Record Keeping

38. Implementing and maintaining an effective records management service depends on knowledge of what records are held, where they are stored, who manages them, in what form(s) they are made accessible, and their relationship to organisational functions (e.g. Finance, Estates, IT, Direct patient care). An information survey or record audit is essential to meeting this requirement. The survey will also help to promote control over the records, and provide valuable data for developing records appraisal and disposal policies and procedures.

39. Paper and electronic record keeping systems should contain descriptive and technical documentation to enable the system to be operated efficiently and the records held in the system to be understood. The documentation should provide an administrative context for effective management of the records.

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

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

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

43. Where an EDRMS is not yet available, electronic documents should be stored on shared, network servers in a clear and meaningful folder structure or "Fileplan" which represents the functions and activities of the organisation or unit. The server should be subject to frequent back-up procedures in line with the NHS Information Security policy. Users should apply the functionality of the relevant software to protect electronic documents against inappropriate amendment (for example, by password protecting documents.) **Please note:** It is almost impossible to fully protect documents in a non-EDRMS environment, or provide full audit and authenticity evidence.

Record Maintenance

44. The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions. The record-keeping system should also address the management of emails, including aspects such as the titling of emails and the handling of email attachments.

45. Storage accommodation for current paper records should be clean and tidy, should prevent damage to the records and provide a safe working environment for staff.

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

47. Equipment used to store current records on all types of media should provide storage that is safe and secure from unauthorised access and meets health and safety and fire regulations, but which also allow maximum accessibility to the information commensurate with its frequency of use.

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

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

Scanning

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

    - the costs of the initial and then any later media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept

    - the need to consult in advance with NHS archivists or the National Archives of Scotland with regard to records which may have archival value, as the value may include the form in which it was created; and

    - the need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the “Code of Practice for Legal Admissibility and evidential weight of information stored electronically” (BIP 0008) and the Document Scanning: Guide to Scanning Business Documents (PD 00 16) which provides guidance to evaluate scanners to user requirements.

51. In order to fully realise business efficiency, organisations should consider securely disposing of paper records that have been copied into electronic format and stored in accordance with appropriate standards and the need to dispose of records in accordance with the retention schedule. Advice should be sought from the organisation's records managers or information governance manager, NHS Scotland archivists or the National Archives for Scotland.

Disclosure and Transfer of Records

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

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

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

55. The mechanisms for transferring records from one organisation to another should also be tailored to the sensitivity of the material contained within the records and the media on which they are held. Information Security staff should be able to advise on appropriate safeguards. The NHS Scotland Information Security policy and standards sets out the requirements for the storage and transmission of corporate and personal records.

56. There are also a range of guidance documents (e.g. the UK Information Commissioner's Use and Disclosure of Health Information) that interpret statutory requirements and there may be staff within organisations that have special expertise in, or can advise on, particular types of disclosure. In particular, organisations should be aware of the Freedom of Information (Scotland) Act 2002 Code of Practice on Records Management November 2003 (laid before the Scottish Parliament on 10th November 2003 pursuant to Section 61(6) of the Freedom of Information (Scotland) Act 2002, and prepared in consultation with the Scottish Information Commissioner and the Keeper of the Records of Scotland). Find out more **here**

Retention and Disposal Arrangements

57. Detailed guidance for retention and disposal of **administrative records** can be found in NHS HDL (2006) 38 'The Management, Retention and Disposal of Administrative Records', which can be accessed from the following **link**

58. Detailed guidance for retention and disposal of **personal health records** can be found in Annex D.

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

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

Appraisal of Records

61. Appraisal refers to the process of determining whether records are worthy of permanent archival preservation. This should be undertaken in consultation with the organisations own Archivist, or one of the three NHS archivists, or with a local authority or university archive where there is an existing relationship. Alternatively advice can be sought from the National Archives of Scotland.

62. Procedures should be put in place in all NHS organisations to ensure that appropriately trained personnel appraise records at the appropriate time. The purpose of this appraisal process is to ensure that the records are examined at the appropriate time to determine whether or not they are worthy of archival preservation, whether they need to be retained for a longer period as they are still in use, or whether they should be destroyed.

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

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

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

Record Closure

66. Records should be closed (i.e. made inactive and transferred to secondary storage) as soon as they have ceased to be in active use other than for reference purposes. An indication that a file of paper records or folder of electronic records has been closed together with the date of closure, should be shown on the record itself as well as noted in the index or database of the

files/folders. Where possible, information on the intended disposal of electronic records should be included in the metadata when the record is created.

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

Record Disposal

68. Each organisation must have a retention/disposal policy that is based on the retention schedules referred to in paragraphs 57 and 58 of this Code of Practice. The policy should be supported by, or linked to the retention schedules, which should cover all records created, including electronic records. Schedules should be arranged based on series or collection of records and should indicate the appropriate disposal action for all records. Schedules should clearly specify the agreed retention periods, which must be based on the retention schedules referred to in paragraphs 57 and 58 of this Code of Practice, for the organisation.

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

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

71. Records (including copies) not selected for archival preservation and which have reached the end of their administrative life should be destroyed in as secure a manner as is appropriate for the level of confidentiality or protective markings they bear. This can be undertaken on site or via an approved contractor. Confidential records should be destroyed in accordance with BS 8470 “Code of Practice on Secure Destruction of Confidential Material”. It is the responsibility of the NHS organisation to ensure that the methods used throughout the destruction process provide appropriate safeguards against the accidental loss or disclosure of the contents of the records. Accordingly, contractors should be required to sign confidentiality undertakings and to produce written certification as proof of destruction.

72. A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the Records Manager, so that the organisation is aware of those records that have been destroyed and are therefore no longer available. Disposal schedules would constitute the basis of such a record.

73. If a record due for destruction is known to be the subject of a request for information, or potential legal action**,** destruction should be delayed until disclosure has taken place or, if the authority has decided not to disclose the information, until the complaint and appeal provisions of the Freedom of Information (Scotland) Act have been exhausted or the legal process completed.

ANNEX A - GLOSSARY OF RECORDS MANAGEMENT TERMS

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

Access

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

Appraisal

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

Archives

Those records that are appraised as having permanent value for evidence of ongoing rights or obligations, for historical or statistical research or as part of the corporate memory of the organisation.

Those records that are appraised as having permanent value. (The National Archives, Records Management Standard RMS 3.1)

Authenticity

An authentic record is one that can be proven:

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

To ensure the authenticity of records, organisations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that records creators are authorised and identified and that records are protected against unauthorised addition, deletion, alteration, use and concealment. (BS ISO 15489-1:2001(E))

CHI Number

The CHI ('Community Health Index') number is a unique numeric identifier, allocated to each patient on first registration with the system. It is a 10-character code consisting of the 6-digit date of birth (DDMMYY), two digits, a 9th digit, which is always even for females and odd for males, and an arithmetical check digit. CHI contains details of all Scottish residents registered with a

General Practitioner. It is a key component in the implementation of an Electronic Patient Record in Scotland.

Classification

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

Conversion (See Also Migration)

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

Corporate Records

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

Current Records

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

Destruction

The process of eliminating or deleting records beyond any possible reconstruction. (BS ISO 15489-1.2001(E))

Disposal

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

Disposition

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

Electronic Record Management System

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

File

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

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

Filing System

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

Health Record

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

Indexing

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

Information Audit

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

Information Survey/Records Audit

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

- Identify where and when records are generated and stored within the organisation and how they are ultimately disposed of;

- Accurately chart the current situation in respect of records storage and retention organisation-wide, to make recommendations on the way forward and the resource implications to meet existing and future demands of the records management function.

Integrity of Records

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

Jointly Held Records

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

Metadata

Contextual information about a record. Data describing context, content and structure of records and their management through time. Metadata is structured information that enables us to describe, locate, control and manage other information.

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

Therefore, metadata should include (amongst other details) elements such as the title, subject and description of a record, the creator and any contributors, the date and format.

For further information, see **The National Archives: Metadata Standard here**

The e-Government Metadata Standard (e-GMS) lays down the elements refinements and encoding schemes to be used by government officers when creating metadata for their information systems. The e-GMS forms part of the e-Government Information Framework (e-GIF).

The e-GMS is required to ensure maximum consistency of metadata across public sector organisations. Find out more **here**

Microform

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

Migration (See Also Conversion)

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

Minutes (Master Copies)

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

Minutes (Reference Copies)

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

NHS Records

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

Health records are the most important tool to support patient care and continuity of that care.

Paper Records

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

Permanent Retention

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

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

Presentation

The transfer to a third party of public records which have been rejected by the Public Record Office but which are not destroyed, under section 3(6) of the Public Records Act 1958.

Preservation

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

Protective Marking

The process of determining security and privacy restrictions on records.

Publication Scheme

A publication scheme is required of all NHS organisations under the Freedom of Information (Scotland) Act. It details information, which is available to the public now or will be in the future,

where it can be obtained from and the format it is available in. Schemes must be approved by the Scottish Information Commissioner and should be reviewed periodically to make sure they are accurate and up to date.

Public Records (Scotland) Act 1937

For information, including the text of the Act, see the National Archives of Scotland **website**:

Records

Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations, or in the transaction of business. (BS ISO 15489.1)

An NHS record is anything, which contains information (in any medium) which has been created or gathered as a result of any aspect of the work of NHS employees - including consultants, agency or casual staff.

Records Management

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

Record Series

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

Record System/Record-Keeping System

An information system which captures, manages and provides access to records through time. (The National Archives, Records Management: Standards and Guidance - Introduction Standards for the management of Government records)

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

Paper and electronic record-keeping systems should contain descriptive and technical documentation to enable the system and the records to be understood and to be operated efficiently, and to provide an administrative context for effective management of the records.

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

Redaction

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

Registration

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

Retention

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

Review

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

Scottish Information Commissioner (See Also UK Information Commissioner)

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

Scottish NHS Archivists

Three NHS Boards in Scotland employ archivists: Grampian (which also provides an archive service to NHS Highland), Lothian, and Glasgow. The funding and managerial arrangements for each of these archives differs, but each collects, lists and preserves corporate and health records of and relating to the NHS organisations and predecessor bodies and institutions in their local area.

NHS organisations which do not employ their own Archivist are welcome to contact one of the four NHS Archivists for advice and information on records management and archiving. See Annex B for further details. These organisations may wish to make their own arrangements with local authority or university archives for the transfer of records selected for permanent preservation; such arrangements require the agreement of the Keeper of the Records of Scotland.

The Health Archives and Records Group (HARG) is a representative body for archivists and records managers working in the health sector, including but not limited to the NHS. Its membership is drawn from across the UK and the Republic of Ireland. It has been an affiliated group of the Society of Archivists' Specialist Repositories Group since 2001. HARG aims to raise the profile of health archives and to improve the level of awareness in the NHS and elsewhere about record-keeping issues.

Tracking

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

Transfer Of Records

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

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

UK Information Commissioner (See Also Scottish Information Commissioner)

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

Weeding

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

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

ANNEX B - RESOURCES TO SUPPORT IMPROVEMENT

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

Information Governance is defined as:-

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

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

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

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

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

The Information Governance Framework also enables the NHS to monitor and manage change by educating staff, developing codes of practice, helping organisations and individuals to understand the requirements of law and ethics in respect of information handling and the consequent need for changes to systems and processes. Furthermore, it enables the NHS to work in partnership with patients and clients by respecting their preferences and choices and addressing their concerns about the use of sensitive, personal information.

The Information Governance Toolkit provides the means by which NHS Boards can assess their compliance against the national information governance standards. The standards can be viewed **here**

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

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

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

Other Reference Material

Good Practice Guidelines for General Practice Electronic Patient Records

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

Quality and Outcomes Framework (QOF)

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

Confidentiality and Disclosure of Information: General Medical Services

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

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

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

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

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

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

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

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

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

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

'The National Archives Guidelines on developing a policy for managing e-mail can be found **here**

Scottish Executive Freedom of Information Act Open Learning Workbook

The Scottish Executive Freedom of Information (Scotland) Act 2002 Open Learning Workbook (2004) can be found **here**

A workbook designed by Masons solicitors on behalf of the Scottish Executive to help public authorities with implementation of Freedom of Information. Modules 5 and 6 deal specifically with records management.

The retention and storage of pathological records and archives

The Royal College of Pathologists: The retention and storage of pathological records and archives (3rd edition, 2005) can be found **here**

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

Recommendations for the retention of pharmacy records

Find this document **here**

Designing and Implementing Records Keeping Systems (BS ISO 15489-1)

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

Information Commissioner CCTV Code of Practice

The ICO has revised its existing code of practice on CCTV to reflect technological developments and changes to the way CCTV is used to monitor individuals. This revised code has now been published and is available **here:**

Information Commissioner: The Use and Disclosure of Health Data

Find this document **here**

Active Records Management: Records Creation

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

e-Government Technical Standards

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

Health and Social Care Data Standards

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

Further information can be obtained from their website **here** and the standards are published in the Health and Social Care Data Dictionary **here**

University of Edinburgh Records Management Section

Access their site **here**

University of Edinburgh file naming conventions

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

Code of Practice for Legal Admissibility and evidential weight of information stored electronically (BIP 0008: 2004 - Copyright BSI)

This **code of practice** has been published in recognition of the growth in electronic information management systems, and the continuing uncertainty about the legal acceptability of information stored on these systems.

Scanning Documentation (P0016: 2001- Copyright BSI)

This **guide** is intended for use by managers responsible for purchasing scanner equipment and in charge of personnel who scan business documents.

Scanning and Document Management in General Practice (May 2006)

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

Educational Material

NHS Scotland Data Protection and Confidentiality Training Package available **here**

Healthcare Information Governance Post-Graduate Education Programme

Unit 2 focuses on **Records Management**

Useful Contacts

Scottish NHS Archives and The National Archives of Scotland

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

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

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

Fiona Watson
Northern Health Services Archives
Victoria Pavilion
Woolmanhill Hospital
Aberdeen
AB25 1LD

Tel: 01224 555562
E-mail: f.watson@nhs.net

For advice on archiving in the NHS Tayside area contact:

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

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

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

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

Archival advice about moving images can be obtained from:

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

Scottish Government eHealth Directorate

Scottish Government eHealth Directorate
St Andrews House
Regent Road
EDINBURGH
EH1 3XD
0131 244 1729

Information Commissioner – Scotland Office

(Data Protection Act 1998)

28 Thistle Street
Edinburgh
EH2 1EN
Tel: 0131 225 6341
Fax: 0131 225 6989
E-mail: Scotland@ico.gsi.gov.uk
Website: http://www.informationcommissioner.gov.uk

Scottish Information Commissioner

(Freedom of Information (Scotland) Act 2002)

Kinburn Castle
Doubledykes Road
St Andrews
Fife
KY16 9DS
Tel: 01334 464610
Fax: 01334 464611
E-mail: enquiries@itspublicknowledge.info
Website: www.itspublicknowledge.info

NHS Scotland Information Governance Programme

Information Governance Team
NHS National Services Scotland
Information Services Division
Area 067
Gyle Square
1 South Gyle Crescent
EDINBURGH
EH12 9EB
Tel: 0131 275 7176
Email: infogov@isd.csa.scot.nhs.uk
Website: www.elib.scot.nhs.uk/infogov

ANNEX C: LEGAL AND PROFESSIONAL OBLIGATIONS

There are a range of legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed. Where necessary, organisations should obtain professional legal advice on the application of these provisions.

A list of key legal and professional obligations covering personal and other information listed in this Annex is below:

Legislation

A

1. Anti-Terrorism, Crime and Security Act 2001
2. The Abortion (Scotland) Regulations 1991
3. The Access to Health Records Act 1990
4. The Access to Medical Reports Act 1988

B

5. The Census (Confidentiality) Act 1991
6. The Computer Misuse Act 1990
7. The Consumer Protection Act (CPA) 1987
8. The Control of Substances Hazardous to Health Regulations 2002
9. The Copyright, Designs and Patents Acts 1990
10. The Crime and Disorder Act 1998
    - Section 115 relates to the disclosure of information

C

11. The Data Protection Act (DPA) 1998
    - The Data Protection (Processing of Sensitive Personal Data) Order 2000
12. The Disability Discrimination Act 1995

D

13. The Electronic Communications Act 2000
14. The Environmental Information (Scotland) Regulations 2004

E

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

F

16. The Gender Recognition (Disclosure of Information) (Scotland) Order 2005

G

17. The Health and Safety at Work Act 1974
18. The Human Fertilisation and Embryology Act 1990, as Amended by the Human Fertilisation and Embryology (Disclosure of Information) Act 1992
19. The Human Rights Act 1998
20. The Human Tissue (Scotland) Act 2006 – Part 1 Section 19 and Part 3
    - (Maintenance of Records and Supply of Information Regarding the Removal and Use of Body Parts) Regulations 2006 (SSI 2006 No. 344)

H

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

I

22. The Mental Health (Care and Treatment) (Scotland) Act 2003

J

23. The Prescription and Limitation (Scotland) Act 1973
24. The Privacy and Electronic Communications (EC Directive) Regulations 2003
25. Public Health Legislation in Scotland
26. The Public Interest Disclosure Act 1998
27. Public Records (Scotland) Act 1937

K

28. The Radioactive Substances Act 1993
    - The High-activity Sealed Radioactive Sources and Orphan Sources Regulations
29. The Re-use of Public Sector Information Regulations 2005

Other Obligations

30. Administrative Law
31. The Blood Safety and Quality Regulations 2005
    - Directive 2002/98/EC of the European Parliament and of the Council of 27 January 2003
    - Commission Directive 2005/61/EC of 30 September 2005
32. The Common Law Duty of Confidentiality
    - NHS Scotland Code of Practice on Protecting Patient Confidentiality
33. Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community Code Relating to Medicinal Products for Human Use

Relevant Standards and Guidelines

34. BSI PD 0016
35. BSI BIP 0008
36. BSI PD 5000
37. BS 4743
38. BS 5454:2000
39. BS ISO/IEC 17799:2005 BS ISO/IEC 27001:2005 BS 7799-2:2005
40. ISO 15489
41. ISO 19005
42. The NHS Scotland Information Governance Toolkit

Professional Codes of Conduct

43. The General Dental Council, Standards for Dental Professionals (06/05)
44. The General Medical Council
45. Health Professionals Council: Standards for Conduct, Performance and Ethics, (01/03) (currently being revised)
46. The Nursing and Midwifery Council Code of Professional Conduct (07/04)
47. The Chartered Society of Physiotherapy: Rules of Professional Conduct

48. Scottish Social Services Council: Codes of Practice for Social Service Workers and Employers
49. Information on Ethical Practice
50. Nursing and Midwifery Council, Record Keeping Guidance (07/07)
51. Midwives' Rules and Standards – NMC Standards (05/04)

Legislation

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

1. Anti-Terrorism, Crime and Security Act 2001

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

2. The Abortion (Scotland) Regulations 1991

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

Records management considerations:

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

3. The Access to Health Records Act 1990

This Act has been repealed to the extent that it now only affects the health records of deceased patients. It applies only to records created since 1 November 1991.

The Act allows access to:

a) the deceased's personal representatives (both executors or administrators) to enable them to carry out their duties; and

b) anyone who has a claim resulting from the death.

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

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

- if disclosure of the information would cause serious harm to the physical or mental health of any person; or

- if disclosure would identify a third party (i.e. not the patient nor a healthcare professional) who has not consented to that disclosure.

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

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

A fee of up to £10 may be charged for providing access to information where all of the records were made more than 40 days before the date of the application. No fee may be charged for providing access to information if the records have been amended or added to in the last 40 days.

Where a copy is supplied, a fee not exceeding the cost of making the copy may be charged. The copy charges should be reasonable, as the doctor or organisation may have to justify them. If applicable, the cost of posting the records may also be charged.

Find out more **here and here**

Records management considerations:

Organisations should have processes that address where and how the records of deceased persons are stored. Secure and environmentally safe storage is vital to ensure that records are maintained in good order and are available if required.

It is essential that organisations put in place processes and procedures to enable the efficient and effective retrieval of such records within the timescales specified by the Act.

4. The Access to Medical Reports Act 1988

The aim of the Act is to allow individuals to see medical reports written about them, for employment or insurance purposes, by a doctor who they usually see in a 'normal' doctor/patient capacity. This right can be exercised either before or after the report is sent.

The chief medical officer of the employer/insurer is the applicant and he/she will send a request for a report to the doctor. The request must be accompanied by a written and signed patient consent.

The patient may view the report by obtaining a photocopy, or by attending the organisation to read the report without taking a copy away. The patient has a right to view the report from the time it is written and has a window to do so before the report is supplied, or he/she may view it after supply for up to six months.

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

- in the opinion of the doctor, viewing the report may cause serious harm to the physical or mental health of the patient; or

- access to the report would disclose third-party information where that third party has not consented to the disclosure.

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

If a patient disagrees with the content of the report, he/she has several options.
He/she can:

- refuse to allow its supply;

- ask the doctor to correct agreed inaccuracies; or

- have a note added addressing the point(s) of disagreement.

Records management considerations:

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

Find out more **here**

5. The Census (Confidentiality) Act 1991

The **Act** makes it a criminal offence to unlawfully disclose personal census information.

If the Registrar-General or any person currently or previously employed or contracted to supply services to him, discloses such information they are committing an offence.

If any person further discloses information knowingly acquired by unlawful disclosure, they are committing an offence.

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

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

The penalties if convicted are:

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

Records management considerations:

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

6. The Computer Misuse Act 1990

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

The offences are:

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

Access is defined in the Act as:

- altering or erasing the computer program or data;
- copying or moving the program or data;
- using the program or data; or
- outputting the program or data from the computer in which it is held (whether by having it displayed or in any other manner).

Unlawful access is committed if the individual intentionally gains access; knowing he is not entitled to do so; and aware he does not have consent to gain access.

The 'further offence' applies if unauthorised access is carried out with intent to commit or cause an offence.

The 'modification' offence applies if an individual does any act causing unlawful modification of computer material and does so in the knowledge that such modification is unlawful, and with the intent to:

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

Records management considerations:

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

See **here** (section 13 covers proceedings in Scotland)

7. The Consumer Protection Act (CPA) 1987

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

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

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

- three years from the date on which the cause of action accrued –effectively, the date the accident took place; or
- three years from the date of knowledge that a cause of action had accrued.

When a person dies, the limitation period runs from:

- three years from the date of death; or
- three years from the date when the personal representative had knowledge that a cause of action had accrued – i.e. the date when they realised that someone was potentially liable for the death.

Records management considerations :

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

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

The **COSHH regulations** specify the eight measures that employers must follow to prevent or limit their employees' exposure to hazardous substances.

The measures are:

- assess the risks;
- decide what precautions are needed;
- prevent or adequately control exposure;
- ensure that control measures are used and maintained;
- monitor the exposure;
- carry out appropriate health surveillance;
- prepare plans and procedures to deal with accidents, incidents and emergencies;
- ensure employees are properly informed, trained and supervised.

Records management considerations:

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

9. The Copyright, Designs and Patents Act 1988

The Act protects the intellectual property of individuals and requires that permission of the owner of the intellectual property is sought before any use of it is made – this includes storage and display on the NHSnet and internet or other electronic information services.

Organisation web pages should not contain, or distribute, text or images to which a third party holds an intellectual property right, without the express written permission of the author. The author may have quoted other people's material and if this is the case, such a third party would also need to give permission.

Records management considerations:

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

10. The Crime and Disorder Act 1998

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

The Anti-Social Behaviour Act (2003) http://www.opsi.gov.uk/acts/acts2003/20030038.htm]amends the 1998 Act, but Part 5 (misuse of air weapons) and Part 10 (general provisions) are the only parts of the act which extend to Scotland.

Records management considerations:

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

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

11. The Data Protection Act (DPA) 1998

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

Personal data is defined as data relating to a living individual that enables him/her to be identified either from that data alone or from that data in conjunction with other information in the data controller's possession. It therefore includes such items of information as an individual's name, address, age, race, religion, gender, and physical, mental or sexual health.

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

a) the racial or ethnic origin of the data subject;

b) his political opinions;

c) his religious beliefs or other beliefs of a similar nature;

d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);

e) his physical or mental health or condition;

f) his sexual life;

g) the commission or alleged commission by him of any offence; or

h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

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

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

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

The Act contains three key strands. These deal with:

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

Notification by a data controller

The data controller is the person who determines how and why personal information is processed. In practice, for NHS organisations the Health Board or practice is the data controller. This means that ultimate responsibility for notification will usually rest with the Chief Executive or GP. The action of notification can be delegated to the most appropriate person within the organisation, for example the head of information management, or the information governance lead.

Notification is the process of informing the Information Commissioner of the fact that processing of personal data is being carried out within a particular organisation. Its purpose is to achieve openness and transparency – notification entries are placed in a register so that members of the public can check the type of processing being carried out by a particular organisation. The notification process involves completion of a form stating the name of the data controller and detailing the types of processing being carried out.

Notification can be done in one of three ways:

1. By completing the online form **here** then printing it and posting to the Information Commissioner;

2. By requesting a notification form **here**

3. By phoning the notification helpline on 01625 545 740

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

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

Compliance with the eight data protection principles

The **eight principles** advocate fairness and openness in the processing of personal information.

The principles state that:

1. personal data shall be processed fairly and lawfully and must be processed in accordance with at least one of the conditions in schedule 2 of the Act. Where the data being processed is sensitive personal information (such as data relating to the physical or mental health of an individual), it must also be processed in accordance with at least one of the conditions in schedule 3 of the Act;

2. personal data shall be obtained only for one or more specified and lawful purpose;

3. personal data shall be adequate, relevant and not excessive for its purpose(s);

4. personal data shall be accurate and where necessary kept up to date;

5. personal data shall not be kept for longer than is necessary for its purpose(s);

6. personal data shall be processed in accordance with the rights of data subjects under this Act;

7. appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

8. personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Records management considerations:

Principle 1

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

To meet the fair processing requirement, individuals must be informed of the fact of processing, including what information will be collected, and how it will be held, recorded, used and shared. The Information Commissioner has issued guidance about the meaning of fair processing which indicates that the processing of personal data for purposes other than those for which the data has been provided may be unfair.

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

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

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

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

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

- for medical purposes by a health professional or by a person who owes the same duty of confidentiality as a health professional;
- where the processing is necessary to protect the vital interests of the patient or another person, i.e. a 'life or death' situation, where consent cannot be obtained or the data controller cannot reasonably be expected to obtain consent;
- where the processing is necessary to protect another person, where consent of the patient has been unreasonably withheld; or
- with the explicit consent of the patient.

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

Principle 2

This principle requires that personal data is not processed in a way that is incompatible with the purpose for which it was obtained. Organisations need to specify how they process information in their notification to the Information Commissioner. They are then required to ensure that all processing carried out is in accordance with those stated purposes. Patients should be fully informed about the reason that their information is required, ie they are not misled into providing information for purposes of which they have no knowledge. If information is obtained for a specific purpose, it must not be used for anything else unless consent is obtained for further uses of the information. For example, identifiable patient information gathered to provide healthcare cannot be used for research unless patient consent is obtained or the information is anonymised. Similarly,

employee information collected to enable salary payment should not be used for purposes unrelated to this, for example marketing of products and services, unless consent is obtained. This principle reinforces the first principle in that it enables patients and the public to find out how a particular organisation states it will use their information.

Principle 3

The aim of this principle is to ensure that organisational records management policies and procedures are in place to support the gathering of relevant, adequate information that is not excessive for its purpose. Organisations should therefore ensure that the information collection procedures in place enable relevant questions to be asked and that training on information collection is made available to all relevant employees.

Systems and processes should be designed to ensure only relevant information is captured and processed.

The organisation should have procedures in place setting out 'need to know' access controls alongside processes that enable conformance to those controls for each member of staff.

Principle 4

To ensure good data quality organisations should follow all the procedures and processes described in the Information Quality Assurance requirements of the Information Governance Toolkit **here**

The requirements describe the procedures and processes that organisations should put in place to ensure that information is accurate and kept up to date.

Principle 5

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

The organisation should put in place arrangements for the closure and disposal (whether destruction or archiving) of records, and secure procedures to prevent unnecessary copying of information.

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

Principle 6

See Rights of the Individual (below).

Principle 7

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

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

Principle 8

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

Rights of the individual

The Data Protection Act gives an individual several rights in relation to the information held about his/ her.

Of particular relevance in a health and social care setting, is the right of individuals to seek access to their records held by the health or social care provider.

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

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

However, the Secretary of State has issued guidance stating that healthcare organisations should endeavour to meet such requests within a 21-day timescale. This is so that Data Protection Act access rights reflect the previous rights contained within the Access to Health Records Act 1990.

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

The right of access is exercisable by the individual:

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

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

If no permanent record is requested, no fee for access may be made to records that contain at least some entries made in the 40-day time period preceding the request, and not, nor intended to be, automatically processed. A fee of £10 may be charged for viewing records that have not been added to in the 40 days prior to the access request.

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

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

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

Records management considerations:

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

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

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

- for the detection and prevention of crime;

- for the protection of members of the public against malpractice, incompetence, mismanagement etc;

- to publicise the fact of malpractice, incompetence, mismanagement etc, for the protection of the public;

- to provide confidential counselling and advice where explicit consent cannot be given nor reasonably obtained, or where the processing must be carried out without explicit consent so as not to prejudice that confidential counselling or advice; or

- to undertake research that does not support measures or decisions with respect to any particular data subject unless the data subject has explicitly consented and does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

Sensitive personal data may also be lawfully processed where:

- the information relates to the data subject or to specific relatives of the data subject and the processing is for the purposes of administering defined insurance business or occupational pensions schemes;

- the processing is carried out by a person authorised under the Registration of Political Parties Act 1998 in the course of their legitimate political business as long as the processing does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person; or

- the processing is necessary for the exercise of any functions conferred on a constable by any rule of law.

Find out more **here**

12. The Disability Discrimination Act 1995

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

Find out more **here**

13. The Electronic Communications Act 2000

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

- legal admissibility for digital signatures;

- registration of cryptography services providers; and

- repeal of and amendments to legislation that places limits on electronic communication and electronic storage of information.

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

Records management considerations:

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

Organisations should be aware of the need to ensure the retention and protection of any cryptographic keys that have been used to protect records, as they may have evidential value over the lifetime of the record.

Find out more **here**

14. The Environmental Information (Scotland) Regulations 2004

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

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

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

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

Find out more **here**

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

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

Records management considerations:

As with the Freedom of Information (Scotland) Act 2002 the organisation needs a robust records management programme. The requirements of the two pieces of legislation are similar so it is advised that organisations deal with requests in a like manner. The main difference is that requests for environmental information need not be in writing.

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

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

For further information, guidance and resources on FOISA see **here**

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

The main features of the Act are:

- a general right of access to recorded information held by public authorities, regardless of the age of the record/document;

- a duty on every public authority to adopt and maintain a publication scheme, which sets out what information will be made available and how it can be accessed; and

- the establishment of the Scottish Information Commissioner, whose role is to promote and to enforce FOISA.

Section 61 of the Act places a duty on Scottish Ministers to issue a Code of Practice on records management. Although compliance with the Code is not obligatory, it provides guidance to all public authorities as to the practice which it would, in the opinion of Scottish Ministers, be desirable for them to follow in connection with the discharge of their functions under the FOI(S)A. Additionally, the Code may be used by the Information Commissioner when deciding whether a public authority has properly dealt with a case (in the event of a complaint).

General right of access

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

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

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

The request for information must:

- be in writing or other permanently recorded format;

- state the name of the applicant and an address for correspondence; and
- describe the information requested.

The applicant can request that information be communicated by:

- a copy in permanent form (or other form acceptable to them, for example on CD-ROM or audio tape);

- inspection of records; or

- a summary or digest of the information held.

Public Authorities must comply to a request promptly; and in any event by not later the 20th working day following receipt of the request and/or the appropriate fee if required.

A public authority need not comply with vexatious requests or repeated requests for information already supplied unless a reasonable period has elapsed between requests.

A fee may be charged by the public authority to cover the costs of locating, retrieving and providing the information requested. This may include:

- staff time, up to a maximum charge of £15 per hour;

- the cost of putting the information into the applicant's requested format, for example CD, or audio tape;

- photocopying and printing costs and;

- postage or other transmission costs.

Where it is estimated that the costs of responding to a request will exceed £600 (the 'upper cost limit') a request for information may be refused. The first £100 of costs may not be charged to the applicant, and thereafter a charge of 10% can be made. The maximum charge is therefore £50. Public authorities are not obliged to make a charge and in many cases may not find it practical to do so.

Publication scheme

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

Publication Schemes must specify:

- the classes of information published, or intended to be published;

- the manner in which publication is, or is intended to be made;

- whether the information is available free of charge or whether payment is required.

Records management considerations:

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

As with Data Protection Act subject access requests, records management staff and procedures are crucial to compliance with this Act. There is a duty imposed on organisations to supply information in a timely fashion – currently within 20 working days. To facilitate this obligation to provide

information within these time limits the organisation must ensure that all employees are aware of how an FOISA application should be progressed and of the requirement to respond to requests quickly.

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

16. The Gender Recognition Act 2004

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

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

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

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

Further information is available from the Department of Constitutional Affairs **here**

Records management considerations:

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

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

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

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

- Specific disclosures in relation to credit reference agencies, insolvency and bankruptcy.

'Medical purposes' includes the purposes of preventative medicine, medical diagnosis and the provision of care and treatment.

Find out more **here**

17. The Health and Safety at Work Act 1974

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

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

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

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

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

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

Records management considerations:

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

18. The Human Fertilisation and Embryology Act 1990, as Amended by The Human Fertilisation and Embryology (Disclosure of Information) Act 1992

The Act is retrospective and applies to information obtained before and after it was passed.

The Act prohibits the disclosure by current and former members and employees of the Human Fertilisation and Embryology Authority of:

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

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

The Government is conducting a review of the whole of this Act and will be holding a public consultation on many aspects of it. This review will include consideration of the confidentiality provisions of the Act, and their compatibility with the Freedom of Information and the Data Protection Acts.

Records management considerations:

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

Find out more **here**

19. The Human Rights Act 1998

The Act became part of UK law on 2 October 2000. It does not contain new rights. It incorporates the European Convention on Human Rights into UK law, allowing an individual to assert their Convention rights in UK courts and tribunals, rather than at the European Court in Strasbourg.

The Act can be used only against a public body, therefore NHS and social care organisations, as public bodies, are subject to the Act. Article 8 of the Act – the right to respect for private and family life – is the most relevant to the health and social care setting.

The Right to Respect for Private and Family Life contains four rights. These are:

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

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

The right to respect for private life

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

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

The Article 8 right reflects the common law duty of confidentiality in that patient information should only be disclosed with that patient's consent. If information is inappropriately disclosed the individual can take legal action for breach against the public body concerned.

Not only must patient information be held confidentially, it must also be held securely. Failure to do so will also breach the right to respect for private life.

The right to respect for family life

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

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

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

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

The right to respect for correspondence

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

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

Interference with an Article 8 right

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

Legitimate social aims are:

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

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

Records management considerations:

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

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

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

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

Requires those removing and receiving body parts to maintain records and supply information to NHSBT and relevant NHS Board. Find out more **here**

> **20.1.** The Human Tissue (Scotland) Act 2006 – A guide to its implications for NHS Scotland. HDL (2006) 46. Find out more **here**

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

The Local Electoral Administration and Registration Services (Scotland) Act 2006 (LEARS Act) introduced changes to the electoral system and registration service in Scotland. Under the Act the General Registrar Office for Scotland was given special powers to share information with other

government departments, including the NHS. The Registrar General creates and maintains a register of individuals from the Register of Births and Deaths and the Adopted Children Register. See Section 57 of the Act for further information. Find out more **here**

22. The Mental Health (Care and Treatment) (Scotland) Act 2003

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

23. The Prescription and Limitation (Scotland) Act 1973

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

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

Records management considerations:

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

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

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

The Regulations set out:

- circumstances under which direct marketing may be carried out;
- duties to safeguard the security of a communications network service;

- limitations on what may be stored or accessed; and
- restrictions on the processing of traffic and location data.

The Regulations are enforced by the UK Information Commissioner. See links **here** and **here**

25. Public Health Legislation in Scotland

The Public Health (Scotland) Act 1897 remains the main legislation, although some parts of this 1897 act have been superseded by more recent legislation. On 26th October 2007 a new Public Health bill was introduced to the Scottish Parliament, further information can be accessed from the following link **here**

In addition information in relation to public health in Scotland can be found from on page 10 and 11 of The Scottish Parliament Information Centre Research Briefing on Public Health in Scotland (2002) can be found **here** and from Chapter 2 of 'Public Health Legislation in Scotland: A Consultation' (Scottish Government, 2005) can be found **here**

The Public Health (Notification of Infectious Diseases) (Scotland) Regulations 1988

Requires medical practitioners to notify their local chief administrative medical officers when they become aware that someone is suffering from a notifiable disease such as chickenpox, food poisoning, legionellosis, mumps, rubella and tetanus. Find out more **here**

26. The Public Interest Disclosure Act 1998

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

Such a disclosure is allowed in the following circumstances:

- where criminal activity or breach of civil law has occurred, is occurring, or is likely to occur;
- where a miscarriage of justice has occurred, is occurring or is likely to occur;
- where health and safety has been, is, or is likely to be compromised;
- where the environment has been, is being or is likely to be damaged; or
- where information indicating evidence of one of the above circumstances is being or is likely to be deliberately concealed.

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

A qualifying disclosure must only be made:

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

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

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

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

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

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

Records management considerations:

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

27. The Public Records (Scotland) Act 1937

Find out more **here**

28. The Radioactive Substances Act 1993

Find out more **here**

The High-activity Sealed Radioactive Sources and Orphan Sources Regulations

The Act applies to organisations that keep, use or dispose of radioactive material or waste. It is supplemented by the High-activity Sealed Radioactive Sources and Orphan Sources Regulations (HASS), which applies additional requirements on organisations that use or dispose of sealed radioactive sources, for example those used for radiography and radiotherapy. Organisations who keep or use radioactive material or sources must obtain a certificate of registration from the Environment Agency, whilst those who dispose of radioactive waste or sources must obtain a certificate of authorisation. Find out more **here**

Records management considerations:

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

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

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

Health Service bodies are required to:

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

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

- an information audit is required for both pieces of legislation to determine the records held and the locations of those records;

- information available for re-use and the terms and conditions of re-use can be included within the organisation's publication scheme (see Freedom of Information (Scotland) Act 2002); and

- if a request is made for access and re-use, the processes need to be coordinated so that the access issue is dealt with before permission to re-use is granted.

OTHER OBLIGATIONS

30. Administrative Law

Administrative law governs the actions of public authorities. According to well-established rules, a public authority must possess the power to carry out what it intends to do. It is also necessary that the power is exercised for the purpose for which it was created or is 'reasonably incidental' to the defined purpose. If not, its action is 'ultra vires' i.e. beyond its lawful powers.

It is important that all NHS bodies are aware of the extent and limitations of their powers and act 'intra vires'. The approach often adopted by Government to address situations where a disclosure of information is prevented by lack of function (the 'ultra vires' rule), is to create, through legislation, new statutory gateways that provide public sector bodies with the appropriate information disclosure function. However, unless such legislation explicitly requires that confidential patient information be disclosed, or provides for common law confidentiality obligations to be set aside, then these obligations must be satisfied prior to information disclosure and use taking place, for example by obtaining explicit patient consent.

Records management considerations:

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

31. Blood Safety and Quality Legislation

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

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

- blood establishments must retain certain information regarding donors, establishment activity and testing of donated blood for a minimum of 15 years (regulation 7);

- blood establishments and hospital blood banks must retain data needed for full traceability for at least 30 years from the point of receipt of the blood or blood component (regulations 8 and 9).

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

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

Find out more **here**

Records management considerations:

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

- allows for identification of each single blood donation and each single blood unit and components thereof; and
- enables full traceability to the donor as well as to the transfusion and the recipient.

That is, the method of recording must unmistakably identify each unique donation and type of blood component, the location at which the donation was received and to whom that donation was given.

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

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

Commission Directive 2005/61/EC of 30 September 2005

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

Data to be retained by blood establishments:

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

Data to be retained by hospital blood banks:

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

lot number of the component, if relevant.

32. The Common Law Duty of Confidentiality

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

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

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

Three circumstances making disclosure of confidential information lawful are:

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

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

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

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

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

Records management considerations:

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

NHSScotland Code of Practice on Protecting Patient Confidentiality

The Code offers detailed guidance on:

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

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

Disclosure after a patient's death:

There are no clear legal obligations of confidentiality that apply to the deceased. Nevertheless it is acknowledged that there is an ethical obligation to the relatives of the deceased in requiring that confidentiality obligations continue to apply.

However, disclosures may be necessary:

- to assist a Procurator Fiscal or other similar officer in connection with an inquest or fatal accident inquiry;
- as part of national confidential enquiries; or
- on death certificates.

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

33. Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community Code Relating to Medicinal Products for Human Use

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

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

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

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

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

RELEVANT STANDARDS AND GUIDELINES

34. BSI PD 0016: Document scanning. Guide to scanning business documents

This guide provides an insight into the processes of document scanning, explain the main features and benefits of different types of scanners and provide guidance to evaluate scanners to user requirements.
Find out more **here**

35. BSI BIP 0008

BSI BIP 0008-1

The current British Standard document relating to 'Legal Admissibility and Evidential Weight of Information Communicated Electronically'. Find out more **here**

BSI BIP 0008-2

The current British Standard document relating to 'Legal Admissibility and Evidential Weight of Information Communicated Electronically'. Find out more **here**

BSI BIP 0008-3

The current British Standard document relating to 'Legal Admissibility and Evidential Weight of Linking Electronic Identity to Documents'. Find out more **here**

36. BSI PD 5000

'Electronic Documents and e-Commerce Transactions as Legally Admissible Evidence': the BSI Code of Practice, PD 5000:1999, enables organisations to demonstrate the authenticity of their electronic documents and e-commerce transactions, so they can be used as legally admissible evidence.

The Standard contains five parts as follows:

- Information Stored Electronically (DISC PD 0008:1999);
- Electronic Communication and Email Policy;
- Identity, Signature and Copyright;
- Using Certification Authorities;
- Using Trusted Third Party Archives.

Find out more **here**

37. BS EN 61010

This series of Standards published between 1988 and 1994 cover the storage, transportation and maintenance of different types of media for use in data processing and information storage. Find out more **here**

38. BS 5454:2000

This makes recommendations for the storage of archival documents. Find out more **here**

39. BS ISO/IEC 17799:2005 BS ISO/IEC 27001:2005 BS7799-2:2005

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

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

40. ISO 15489

This is the international records management standard and is about best practice in records management. Find out more **here**

41. ISO 19005 – Document Management

This Standard provides for organisations to archive documents electronically for long-term preservation. Find out more **here**

42. The NHS Scotland Information Governance Toolkit

Information Governance is the process by which NHS Boards ensure that the data and information over which they have stewardship is dealt with legally, securely, effectively and efficiently. The Toolkit underpins the Information Governance Standards outlined in *'NHS Quality Improvement Scotland (NHS QIS) Clinical Governance and Risk Management Standards'*.

All NHS Boards are required to review their performance against the standards each quarter which cover all facets of information governance including:

- Data Protection Act 1998;
- Freedom of Information (Scotland) Act 2002;
- The NHSScotland Code of Practice on Protecting Patient Confidentiality;
- Corporate and Health Records Management;
- Information Quality Assurance;
- Information Security;

- Information Governance Management.

The reports generated in this process will be shared with NHS Quality Improvement Scotland to inform the Clinical Governance and Risk Management Standards peer review visits. Find out more **here**

Professional Codes of Conduct

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

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

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

43. The General Dental Council, Standards for Dental Professionals (06/05)

The GDC **guidance** explains the standards the GDC expects of dental professionals:

44. The General Medical Council

Core GMC guidance **here**

New guidance for 0-18 years is available **here**

45. Health Professionals Council: Standards for Conduct, Performance and Ethics, (01/03)

Document **here** explaining the standards of conduct, performance and ethics that registrants and prospective registrants must keep to. The document also gives an idea of the kind of behaviour that is likely to lead to a fitness to practise hearing.

46. The Nursing and Midwifery Council Code of Professional Conduct

The **NMC Standards 07.04** informs the professions of the standard of professional conduct required of them in the exercise of their professional accountability and practice.

Nursing and Midwifery Council (NMC) Standards for Medicine Management

Replaces the '*Guidelines for the administration of medicines*' which were revised in March 2004 *t*o bring it into line with changes brought about by the Nursing and Midwifery Order 2001. Includes records management guidance on transcribing medication from one "direction to supply or administer" to another form of"direction to supply or administer" and storage of medication and associated records.

47. The Chartered Society of Physiotherapy: Rules of Professional Conduct

Find out more **here**

48. Scottish Social Services Council: Codes of Practice for Social Service Workers and Employers

Find out more **here**

49. Information on ethical practice

This can be obtained from the British Medical Association **here**

50. Nursing and Midwifery Council (NMC) Record Keeping Guidance

Guidelines **here** prepared by the NMC on records and record-keeping practices for nurses and midwives.

51. Midwives' Rules and Standards – NMC Standards

The Nursing and Midwifery Order 2001 requires the NMC to set rules and standards for midwifery. The rules and standards document provides guidance on the interpretation of these rules and standards and includes record keeping.

Find out more **here**

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

1. Introduction

1.1. Scope of Schedule

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

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

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

The Annex does not include minimum retention periods for administrative records commonly found within NHS organisations. Guidance on corporate (i.e. administrative, non-health) records is given in **NHS HDL (2006) 28** 'The Management, Retention and Disposal of Administrative Records'.

1.2. Responsibilities and Decision Making

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

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

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

1.3. Retention Periods

Each organisation must produce its own retention schedule, specifying the locally agreed retention periods, in the light of its own internal requirements. Organisations must not apply to any records a shorter retention period than the minimum set out in this schedule, but there may be circumstances in which they need to apply a longer retention period. Organisations should ensure that they are able to justify, particularly in terms of the Data Protection Act when applicable, the retention of records for longer than the minimum period set out in this schedule.

NHS Boards and GPs as producers of products and equipment, are affected by the provisions of the Consumer Protection Act 1987 covering the liability of producers for defective products. They may also be liable in certain circumstances as suppliers and users of products. An obligation for liability lasts for 10 years and within this period the Prescription and Limitation (Scotland) Act 1973, as amended by the Consumer Protection Act 1987, provides that the pursuer must commence any action within 3 years' from the date on which the pursuer was aware of the defect and aware that the damage was caused by the defect. This means that if a defective product was likely to have affected the health of a patient, then the patient's record would have to be retained for at least 13 years'. It will be for Boards and GPs to make their own judgement in such cases on whether any health records should be retained for this minimum period in order to defend any action brought under the Consumer Protection Act 1987

Organisations should ensure that they have mechanisms in place to identify records for which the appropriate minimum retention period has expired, in line with the 5th principle of the Data Protection Act 1998. It is acknowledged that organizations will have different mechanisms available to them in order to do this, and that these may vary depending on the medium on which the record is held. In relation to paper records in particular, it is acknowledged that organisations may 'batch' records together e.g. on an annual basis, in order to make disposal decisions. In such instances one approach to the calculation of minimum retention periods would be to base it on the beginning of the year after the last date on the record. For example, a file in which the first entry is in February 2001 and the last in September 2004, and for which the retention period is six years, would be kept in its entirety at least until the beginning of 2011.

1.4. Disposal and Destruction of Personal Health Records

1.4.1. Decision Making

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

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

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

storage, it is recommended that the views of the profession's local representatives should be obtained.

1.4.2 Disposal and Destruction

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

1. **Review**: records may need to be kept for longer than the minimum retention period due to ongoing administrative and/ or clinical need. As part of the review, the organisation should have regard to the fifth principle of the Data Protection Act 1998, which requires that personal data is not kept longer than is necessary.

   If it is decided that the records should be retained for a period longer than the minimum the internal retention schedules will need to be amended accordingly and a further review date set. Otherwise, one of the following will apply:

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

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

1.5. Archives

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

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

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

2. Interpretation of the Schedule

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

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

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

Find out more **here**

The Schedule is organised into a table with 3 headings:

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

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

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

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

Record Type	***Minimum NHS Retention Period***
Adult	6 years after date of last entry or 3 years after death if earlier
All types of records relating to Children and young people (including children's and young person's Mental Health Records)	Retain until the patient's 25th birthday or 26th if young person was 17 at conclusion of treatment, or 3 years after death. If the illness or death could have potential relevance to adult conditions or have genetic implications, the advice of clinicians should be sought as to whether to retain for a longer period.
Mentally disordered person (within the meaning of any Mental Health Act)	20 years after date of last contact between the patient/ client/ service user and any health/ care professional employed by the mental health provider, or 3 years after the death of the patient/ client/ service user if sooner and the patient died while in the care of the organisation. N.B. NHS organisations may wish to keep mental health records for up to 30 years before review. Records must be kept as complete records for the first 20 years in accordance with this retention schedule but records may then be summarised and kept in summary format for the additional 10-year period. Social services records are retained for a longer period. Where there is a joint mental health and social care record, the higher of the two retention periods should be adopted. When the records come to the end of their retention period, they must be reviewed and not automatically destroyed. Such a review should take into account any genetic implications of the patient's illness. If it is decided to retain the records, they should be subject to regular review.

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

3. Health Records Retention Schedule

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
A&E records (where these are stored separately from the main patient record)	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
A&E registers (where they exist in paper format)	8 years after the year to which they relate	Likely to have archival value- see Note 1 (page 100)
Abortion – Certificates set out in Schedule 1 to the Abortion (Scotland) Regulations 1991	3 years beginning with the date of the termination	
Admission books (where they exist in paper format)	8 years after the last entry	Likely to have archival value- see Note 1 (page 100)
Ambulance records – patient identifiable component (including paramedic records made on behalf of the Ambulance Service)	7 years	
Asylum seekers and refugees (NHS personal health record – patient held record)	Special NHS record- patient held, no requirement on the NHS to retain	
Audiology records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
Birth registers (ie register of births kept by the hospital)	2 years	Likely to have archival value- see Note 1 (page 100)
Body release forms	2 years	
Breast screening Xrays	8 years	
Cervical screening slides	10 years	
Chaplaincy records	2 years	Likely to have archival

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
		value- see Note 1 (page 100)
Child and family guidance	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
Child Protection Register (records relating to)	Retain until the patient's 26th birthday	
Clinical audit records	5 years	
Clinical psychology	30 years	
Clinical trials of investigational medicinal products – health records of participants that are the source data for the trial	**For trials to be included in regulatory submissions:** At least 2 years after the last approval of a marketing application in the EU. These documents should be retained for a longer period, however, if required by the applicable regulatory requirement(s) or by agreement with the Sponsor. It is the responsibility of the Sponsor/someone on behalf of the Sponsor to inform the investigator/institution as to when these documents no longer need to be retained. **For trials which are not to be used in regulatory submissions:** At least 5 years after completion of the trial. These documents should be retained for a longer period if required by the applicable regulatory requirement(s), the Sponsor or the funder of the trial In either case, if the period appropriate to the specialty is greater, this is the minimum retention period.	See Note 1 (page 100)
Counselling records	30 years	See Note 1 (page 100)
Death – Cause of, Certificate counterfoils	2 years	
Death registers – i.e. register of deaths kept	2 years	Likely to have archival value- see Note 1 (page

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
by the hospital, where they exist in paper format		100)
Dental epidemiological surveys	30 years	
Dental, ophthalmic and auditory screening records	Adults: 11 years Children: 11 years, or up to 25th birthday, whichever is the longer	
Diaries – health visitors and district nurses	2 years after end of year to which diary relates. Patient relevant information should be transferred to the patient record.	It is not good practice to record patient identifiable information in diaries.
Dietetic and nutrition	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
Discharge books (where they exist in paper format)	8 years after the last entry	Likely to have archival value- see Note 1 (page 100)
District nursing records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
Donor records (blood and tissue)	30 years post transplantation	See Note 1 (page 100)
Family planning records	10 years after the closure of the case For children retain until their 25th birthday	
Forensic medicine records (including pathology, toxicology, haematology, dentistry, DNA testing, post mortems forming part of the Procurator Fiscal's report, and human tissue kept as part of the forensic	For postmortem records which form part of the Procurator Fiscal's report, approval should be sought from the PF for a copy of the report to be incorporated in the patient's notes, which should then be kept in the pathology laboratory, and then reviewed. All other records retain for 30 years.	See Note 1 (page 100)

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
record) See also Human tissue, Post mortem registers		
Genetic records	30 years from date of last attendance.	See Note 1 (page 100)
Genito Urinary Medicine (GUM)	Store according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
GP records, including medical records relating to HM Armed Forces	Retain for the lifetime of the patient and for 3 years after their death. **Records relating to those serving in HM Armed Forces -** The Ministry of Defence (MoD) retains a copy of the records relating to service medical history. The patient may request a copy of these under the Data Protection Act (DPA), and may, if they choose, give them to their GP. GPs should also receive summary records when ex-Service personnel register with them. What GPs do with them is a matter for their professional judgement, taking into account clinical need and Data Protection Act requirements- they should not, for example, retain information that is not relevant to their clinical care of the patient. GP records of serving military personnel in existence prior to them enlisting must not be destroyed. Following the death of the patient the records should be retained for 3 years. ***Electronic Patient Records (EPRs)- GP only-** must not be destroyed, or deleted, for the foreseeable future	*The rationale for this is explained in 'SCIMP Good Practice Guidelines for General Practice Electronic Patient Records - **section 6.1'**

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
Health visitor records	10 years Records relating to children should be retained until their 25th birthday	
Homicide/'serious untoward incident' records	30 years	See Note 1 (page 100)
Hospital acquired infection records	6 years	
Human fertilisation records, including embryology records	**Treatment Centres** 1. If a live child is not born, records should be kept for at least 8 years after conclusion of treatment 2. If a live child is born, records shall be kept for at least 25 years after the child's birth 3. If there is no evidence whether a child was born or not, records must be kept for at least 50 years after the information was first recorded **Storage Centres** Where gametes etc have been used in research, records must be kept for at least 50 years after the information was first recorded. **Research Centres** Records are to be kept for 3 years from the date of final report of results/ conclusions to Human Fertilisation and Embryology Authority (HFEA)	See Note 1 (page 100)
Human tissue (within the meaning of the Human Tissue (Scotland) Act 2006) (see Forensic medicine above)	For post mortem records which form part of the Procurator Fiscal's report, approval should be sought from the Procurator Fiscal for a copy of the report to be incorporated in the patient's notes, which should then be	See Note 1 (page 100)

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
	kept in line with the specialty, and then reviewed.	
Intensive Care Unit charts	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
Joint replacement records	For joint replacement surgery the revision of a primary replacement may be required after 10 years to identify which prosthesis was used. Only need to retain minimum of notes with specific information about the prosthesis.	See Note 1 (page 100)
Learning difficulties – (records of patients with)	Retain for 3 years after the death of the individual.	
Macmillan (cancer care) patient records – community and acute	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Maternity (all obstetric and midwifery records, including those of episodes of maternity care that end in stillbirth or where the child later dies)	25 years after the birth of the last child	
Medical illustrations (see Photographs below)	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Mentally disordered persons (within the meaning of any Mental Health Act)	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Microfilm/microfiche records relating to patient care	Retain according to the standard minimum retention period appropriate to the patient/ specialty	May have archival value- see Note 1 (page 100)

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
	(see Above)	
Midwifery records	25 years after the birth of the last child	
Mortuary registers (where they exist in paper format)	10 years	See note 1 (page 100)
Music therapy records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Neonatal screening records	25 years	
Notifiable diseases book	6 years	
Occupational Health Records (staff)	6 years after termination of employment	
Health Records for classified persons under medical surveillance	50 years from the date of the last entry or age 75, whichever is the longer	See Note 1 (page 100)
Personal exposure of an identifiable employee monitoring record	40 years from exposure date	See Note 1 (page 100)
Personnel health records under occupational surveillance	40 years from last entry on the record	See Note 1 (page 100)
Radiation dose records for classified persons	50 years from the date of the last entry or age 75, whichever is the longer	See Note 1 (page 100)
Occupational therapy records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Oncology (including radiotherapy)	30 years	See Note 1 (page 100)

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
	N.B. Records should be retained on a computer database if possible. Also consider the need for permanent preservation for research purposes.	
Operating theatre registers	8 years after the year to which they relate	Likely to have archival value- see Note 1 (page 100)
Orthoptic records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Out of hours records (GP cover), including video, DVD and tape voice recordings	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Outpatient lists (where they exist in paper format)	2 years after the year to which they relate	
Parent held records	There should be a copy kept at the NHS organisation responsible for delivering that care and compiling the record of the care. The records should then be retained until the patient's 25th birthday, or 26th birthday if the young person was 17 at the conclusion of treatment, or 3 years after death	
Pathology records		
Documents, electronic and paper records		
Accreditation documents; records of inspections	10 years or until superseded	
Batch records results	10 years	
Bound copies of reports/records, if made	30 years	
Day books and other records of specimens	2 calendar years	

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
received by a laboratory		
Equipment/ instruments maintenance logs, records of service inspections Procurement, use, modification and supply records relevant to production of products (diagnostics) or equipment	Lifetime of equipment 11 years	
External quality control records	2 years	
Internal quality control records	10 years	
Lab file cards or other working records of test results for named patients	2 calendar years	
Near-patient test data	Result in patient record, log retained for lifetime of instrument	
Pathological archive/museum catalogues	30 years, subject to consent	
Records of telephoned reports	2 calendar years	
Records relating to investigation or storage of specimens relevant to organ transplantation, semen or ova	30 years if not held with health record	
Reports, copies Post mortem reports	6 months Held in the patient's health record for 8 years after the patient's death	
Request forms that are	1 week after report received by	

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
not a unique record	requestor	
Request forms that contain clinical information not readily available in the health record	30 years	
Standard operating procedures (current and old)	30 years	
Specimens and preparations		
Blocks for electron microscopy	30 years	
Electrophoretic strips and immunofixation plates	5 years unless digital images taken, in which case 2 years and stored as a photographic record	
Foetal serum	30 years	
Frozen tissue for immediate histological assessment (frozen section)	Stained microscope slides- 10 years Residual tissue- kept as fixed specimen once frozen section complete	
Frozen tissues or cells for histochemical or molecular genetic analysis	10 years	
Grids for electron microscopy	10 years	
Human DNA	4 weeks after final report for diagnostic specimens. 30 years for family studies for genetic disorders (consent required)	
Microbiological cultures	24-28 days after final report of a positive culture issued. 7 days for certain specified cultures- see RCPath document	
Museum specimens (teaching collections)	Permanently. Consent of the relative is required if it is tissue	

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
Stained slides	obtained through post mortem Depends on the purpose of the slide- see RCPath **document** for further details	
Newborn blood spot screening cards Body fluids/ aspirates/ swabs	5 years- parents should be alerted to the possibility of contact from researchers after this period and a record kept of their consent to contact response 48 hours after the final report issued by lab	
Paraffin blocks	30 years and then appraisal for archival value	
Records relating to donor or recipient sera	11 years post transplant	
Serum from first pregnancy booking visit	1 year	
Wet tissue (representative aliquot or whole tissue or organ)	4 weeks after final report for surgical specimens	
Whole blood samples, for full blood count	24 hours	
Transfusion laboratories		
Annual reports (where required by EU directive)	15 years	
Autopsy reports, specimens, archive material and other where the deceased has been the subject of Procurator Fiscals autopsy	These are Procurator Fiscal's records- copies may only be lodged on the health record with the PF's permission.	

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
Blood bank register, blood component audit trail and fates	30 years to allow full traceability of all blood products used.	
Blood for grouping, antibody screening and saving and/or cross-matching	1 week at 4˚ C	
Forensic material – criminal cases	Permanently- not part of the health record	
Refrigeration and freezer charts	11 years	
Request forms for grouping, antibody screening and crossmatching	1 month	
Results of grouping, antibody screening and other blood transfusion-related tests	30 years to allow full traceability of all blood products used	
Separated serum/plasma, stored for transfusion purposes	Up to 6 months	
Storage of material following analyses of nucleic acids	30 years See RCPath **document** for further guidance	Currently under review
Worksheets	30 years to allow full traceability of all blood products used	
end of Pathology records		
Patient held records	At the end of an episode of care the NHS organisation responsible for delivering that care and compiling the record of the care must make appropriate arrangements to retrieve patient-held records. The records should then be retained for the period appropriate to the	

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
	patient/ specialty (see Above).	
Pharmacy Records		
Prescriptions		
Chemotherapy	2 years after last treatment	
Clinical drug trials (non-sponsored)	2 years after completion of trial	
GP10, TTO's, outpatient, private	2 years	N.B. Inpatient prescriptions held as part of health record.
Parenteral nutrition	2 years	Original valid prescription to be held with the health record.
Unlicensed medicines dispensing record	5 years	
Worksheets		
Raw material request and control forms	5 years	
Resuscitation box	1 year after the expiry of the longest data item Applies only to re-packaged items.	
Chemotherapy, aseptics worksheets, parenteral nutrition, production batch records	5 years	NHS organisations should be aware of product liability which means that if a defective product was likely to have affected the health of a patient, the patient's record would have to be retained for at least 13 years (Prescription and Limitation (Scotland) Act 1973 as amended by the Consumer Protection Act 1987)
Paediatric	As per Children and Young People (see Above)	
Quality Assurance		
Environmental monitoring results	1 year after expiry date of products	

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
Equipment validation	Lifetime of the equipment	
QC Documentation, certificates of analysis	5 years or 1 year after expiry of batch (whichever is longer)	
Refrigerator temperature	1 year	Refrigerator records to be retained for the life of any product stored therein
Standard operating procedures	5 years after superseded by revised version	
Orders		
Invoices	6 years	
Order and delivery notes, requisition sheets, old order books	Current financial year plus one	
Picking tickets/ delivery notes	3 months	
Ward Pharmacy requests	1 year	
Controlled Drugs		
Controlled drug destruction records (pharmacy and ward based)	2 years	
Controlled drug prescriptions (TTOs/OP)	2 years	
Controlled drug order books, ward orders and requisitions	2 years	
Controlled drug registers (pharmacy and ward based)	2 years	
Other		
Medicines information enquiry	10 years	

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
(end of Pharmacy)		
Photographs (where the photograph refers to a particular patient it should be treated as part of the health record)	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Physiotherapy records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Podiatry records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Post mortem records (see Pathology records)		
Post mortem registers (where they exist in paper format)	30 years	Likely to have archival value- see Note 1 (page 100)
Private patient records admitted under section 57 of the National Health Service (Scotland) Act 1978 or section 5 of the National Health Service (Scotland) Act 1947 (now repealed)	It would be appropriate for authorities to retain these according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
Psychology records	30 years	See Note 1 (page 100)
Records/documents related to any litigation	As advised by the organisation's legal advisor. All records to be reviewed.	See Note 1 (page 100)
Records of destruction of individual health records (case notes) and other health related records contained in this retention schedule (in manual or computer	Permanently	See Note 1 (page 100)

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
format)		
Research records 1. Other than clinical trials of investigational medicinal products, health records of participants that are the source data for the research	30 years	See Note 1 (page 100) Review patient identifiable records every 5 years to see if they need to be retained or if their identifiability could be reduced.
2. Research records and research databases (not patient specific)	**Clinical trials of investigational medicinal products** At least 2 years after the last approval of a marketing application in the EU. These documents should be retained for a longer period, however, if required by the applicable regulatory requirement(s) or by agreement with the sponsor. It is the responsibility of the sponsor/ someone on behalf of the sponsor to inform the investigator/ institution as to when these documents no longer need retained. **Research records other than for clinical trials of investigational medicinal products** As above.	See Note 1 (page 100)
Scanned records relating to patient care	Retain in main records and retain for the period of time according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
School health records (see Children and young people)	Retain in Child Health Records	
Speech and language therapy records	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	
Telemedicine records	Retain according to the standard	

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
(see also Video records)	minimum retention period appropriate to the patient/ specialty (see above)	
Transplantation records	Records not otherwise kept or issued to patient, records that relate to investigations or storage of specimens relevant to organ transplantation should be kept for 3 years	See Note 1 (page 100)
Ultrasound records (e.g. vascular, obstetric)	Retain according to the standard minimum retention period appropriate to the patient/ specialty (see Above)	
Video records/ voice recordings relating to patient care/video-conferencing records (see also Telemedicine records and Out of hours records)	8 years subject to the following exceptions: **Children and Young People**- Records must be kept until the patient's 25th birthday, of the patient was 17 at the conclusion of treatment until their 26th birthday, or until 3 years after the patient's death if sooner. **Maternity**- 25 years **Mentally disordered persons**- Records should be kept for 20 years after the date of last contact between patient/ client/ service user and any healthcare professional or 3 years after the patient's death if sooner. **Cancer patients**- Records should be kept until 8 years after the conclusion of treatment, especially if surgery was involved. The Royal College of Radiologists has recommended that such records be kept permanently where chemotherapy and/ or radiotherapy was given.	The teaching and historical value of such recordings should be considered, especially where innovative procedures or unusual conditions are involved. Video/ video-conferencing records should be either permanently archived or permanently destroyed by shredding or incineration (having due regard to the need to maintain patient confidentiality)
Ward registers, including daily bed returns (where they	2 years after the year to which they relate	Likely to have archival value- see Note 1 (page 100)

TYPE OF HEALTH RECORD	MINIMUM RETENTION PERIOD	NOTE
exist in paper format)		
Xray films (excluding PACS images)	The minimum retention period for these can continue to be determined locally by the NHS organisation responsible. In setting the minimum retention period, appropriate recognition should be given to current professional guidance, clinical need, special interest groups, cost of storage and the availability of storage space.	
Xray – PACS images	**National:** PACS images captured as part of the national PACS programme are stored in a central national archive in accordance with the National PACS for Scotland Image Retention/ Storage Policy, which is subject to annual review by the PACS Clinical Advisory Group. **Local:** Locally set minimum retention periods can continue to apply to PACS images that are not captured as part of the national PACS programme.	As eHealth strategic developments progress, this guidance, along with that for other record types affected, will be reviewed.
Xray registers (where they exist in paper format)	30 years	Likely to have archival value- see Note 1 (page 100)
Xray reports (including reports for all imaging modalities)	To be considered as part of the patient record. Retain according to the standard minimum retention period appropriate to the patient/ specialty (see above)	

Note 1 - record is likely to have permanent research and historical value, consult NHS archivist or National Archives of Scotland.

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

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

Joint Position on the Retention of Maternity Records

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

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

3. Local level decision making with administrators on behalf of the health authority must include proper professional representation when agreeing policy about essential maternity records. 'Proper professional' in this context should mean a senior medical practitioner(s) concerned in the direct clinical provision of maternity and neonatal services and a senior practising midwife.

4. Local policy should clearly specify particular records to be retained AND include detail regarding transfer of records, and needs for the final collation of the records for storage. For example, the necessity for inclusion of community midwifery records.

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

List of Maternity Records to be retained

6. Maternity Records retained should include the following:
   6.1. documents recording booking data and pre-pregnancy records where appropriate;

   6.2. documentation recording subsequent antenatal visits and examinations;
   6.3. antenatal inpatient records;

   6.4. clinical test results including ultrasonic scans, alphafeto protein and chorionic villus sampling;
   6.5. blood test reports;
   6.6. all intrapartum records to include initial assessment, partograph and associated records including cardiotocographs;

   6.7. drug prescription and administration records;

6.8. postnatal records including documents relating to the care of mother and baby, in both the hospital and community settings.

ANNEX E – NHSSCOTLAND PERSONAL HEALTH RECORDS MANAGEMENT POLICY FOR NHS BOARDS

***Please note** - this annex was developed by a subgroup of The Health Records Forum, and has been the subject of a recent consultation. It has been included in this overarching Code of Practice to provide further advice and support to NHS Boards in the development of local health record policies. It is recognised by the Scottish Government eHealth directorate as a useful tool for Boards in helping them meet their records management obligations.*

1. HEALTH RECORDS MANAGEMENT POLICY

1.1 Introduction

(Insert name of NHS Board) takes its responsibility towards patient confidentiality seriously and patient records should always be held in a secure environment and accessed on a need to know basis.

Health records are a valuable resource because of the information they contain. They are essential to the delivery of high quality evidence based health care. Health records are contemporaneous and form the basis for the organisation's accountability for clinical care. They are evidential documents and as such must comply with legislative requirements, professional standards and guidelines. It is essential to the operation of the organisation to be able to identify and locate information that is critical for current decision making and to determine which policies and procedures are followed during the delivery of clinical care.

Health records management is the process of managing records throughout their life cycle, from their creation, usage, maintenance and storage to their ultimate destruction or permanent preservation.

Legislation has a significant effect on record keeping arrangements in NHS organisations. NHS Scotland must ensure that health records management policies and procedures are fully compliant with legislation and government policy on the management of information, namely:

- Public Records (Scotland) Act 1937;
- Medical Reports Act 1988;
- The Computer Misuse Act 1990;
- Access to Health Records Act 1990;
- Data Protection Act 1998;
- Human Rights Act 2000;
- Scottish Government Records Management NHS Code of Practice (Scotland);
- Quality Improvement Scotland - Standards for Record Keeping;

- Information Governance Standards;
- National eHealth Strategy

This policy should be read in conjunction with the organisation's Health Records Management Strategy, which sets out how the policy requirements will be delivered.

1.2. Scope of the Policy

This policy sets out best practice for in creating, using, retaining and disposing of health records. It applies to health records in all formats, of all types and in all locations used:

- to support patient care and the continuity of care;
- to support day to day corporate activities which underpin delivery of care;
- to support evidence based practice;
- to support epidemiology;
- to meet legal requirements and regulatory requirements;
- to assist medical and other audits;
- to support improvements in clinical effectiveness through research.

1.3. Definition of a Health Record

A health record is anything that contains information, which has been created or gathered as a result of any aspect of the delivery of patient care, including:

- personal health records (electronic, microfilm and paper based);
- radiology and imaging reports, photographs and other images;
- audio and video tapes, cassettes, CD ROM etc;
- computer databases, output and disks etc and all other electronic records;
- material intended for short term or transitory use including notes and "spare copies of documents".

This list is not exhaustive.

The health record should be constructed to contain sufficient information to identify the patient, provide a clinical history, details of investigations, treatment and medication.

1.4. Aims of Health Records Management System

The aim of this health records policy is to ensure that procedures are in place to bring together the health professionals and accurate, relevant, reliable patient documentation at the correct time and place to support patient care. In achieving this aim, all NHS Scotland employees should fulfil statutory and other legal requirements, ensuring patient safety and safe custody and confidentiality of patient information at all times.

The aims of our health records management system are to ensure that:

- **health records are available when** needed – from which the Health Board is able to form a reconstruction of activities or events that have taken place;

- **health records can be accessed** – health records and the information within them can be located and displayed in a way consistent with the records' initial use and that the current version is identified where multiple versions exist;

- **health records can be interpreted** – the context of the record can be interpreted: who created or added to the health record and when, during which business process, and how the health record is related to other health records;

- **health records can be trusted** – the health record reliably represents the information that was actually used in or created by the business process, and the records integrity and authenticity can be demonstrated;

- **health records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the health record is needed, perhaps permanently despite changes of format;

- **health records are secure** – from unauthorised and inadvertent alteration and erasure. Access and disclosure are properly controlled and audit trails will track all use and changes to ensure that health records are held in a robust format which remains readable for as long as they are required;

- **health records are retained and disposed of appropriately** – using consistent documented retention and disposal procedures, which include provision of appraisal and permanent preservation for health records with archival value;

- **staff are trained** – all staff are made aware of their responsibilities for health record keeping and management.

1.5. Health Records Life Cycle Process

Health records are confidential documents and should be clearly identifiable, accessible and retrievable. They should be authentic, meaningful, authoritative, adequate for their purpose and correctly reflect what was communicated, decided or done. They should be unalterable and after an action has occurred nothing from the health record should be deleted or altered. Information added to an existing hard copy health record should be signed and dated. Health records systems should be secure and their creation, management, storage and disposal should comply with current legislation.

1.5.1. Creation

A comprehensive health record is created and maintained for every patient attending health services to provide an up to date and chronological account of the patient's care.

- patient demographic data for each registration should be recorded on the master patient index of the patient administration or departmental patient management system. The minimum patient demographic data should include surname, forename, sex, date of birth, home address, postcode, Community Health Index (CHI) number and/or departmental number;

- the organisation should use the CHI number as the unique patient identifier;

- where there is more than one local identifier or case record per patient, a system should be in place to ensure that the existence of all other health records is known at all times;

- paper health records have a standard case record folder constructed of robust material to withstand handling and transport and with secure anchorage points to prevent loss or damage to documents. There should be no inside pockets or flaps as these can lead to misfiling or loss of documents;

- there is a method for indicating alert or risk factors which is used consistently in all personal health records, with a designated place for healthcare professionals to record actual or suspected clinical alerts and hazards which are signed and dated. There may be an indicator on the outside of the folder but the confidential detail should be placed inside the folder;

- there is a locally agreed format for filing of information within the health record which facilitates ease of access to all clinical information. Clear instructions regarding the order of filing should be contained within the folder or printed on the divider(s). Documents should be viewable in chronological order reflecting the continuum of patient care;

- machine generated reports and recordings, e.g. CTG, ECG and laboratory reports, are securely stored using a method that will minimise deterioration;

- there are dated documented procedures for the management of electronic health records;

- all electronic health record information systems are password protected and passwords are changed at regular intervals.

1.5.2. Storage

Health records storage areas should provide a safe working environment with secure storage that allows health records to be retrieved at all times. These areas should only be accessible to authorised staff.

- health records storage areas and office accommodation conform to all current legislation and guidance regarding health and safety;

- regular risk assessments are undertaken in line with the organisation's risk management strategy;

- racking for storage of health records is stable, of strong enough construction to support the weight of health records and complies with current health and safety regulations;

- there are safety step ladders and safety stools appropriate to the number of staff employed/size and use of the health records storage area;

- there is a documented protocol for safe manual and object handling practices. All staff are fully trained in related manual handling;

- there is a mechanism to ensure that all equipment used in the department conforms to appropriate legislation and a record of equipment checks is kept;

- access to health records storage areas is restricted to authorised personnel only. Health records should not be accessible to unauthorised persons nor left for any period where they might be accessed by unauthorised persons. The keys/access codes/access pass to storage areas that are locked are available to authorised staff at all times to facilitate retrieval of health records;

- health records storage areas must be able to accommodate current needs and annual growth of health records. The health records collection inventory demonstrates how this will be achieved;

- health records are stored securely when located in clinical areas or offices and arrangements are in place to facilitate retrieval of health records when required.

1.5.3. Management

Maintaining proper health records is vital to patient care. A comprehensive health record should be maintained for every patient. Each health records system should have well defined procedures for the ongoing management of the health record from initiation to final disposal in accordance with current legislation.

- whenever possible, separate areas are maintained for current and non current health records in use within the organisation;

- there are documented procedures for the safe storage and retrieval of health records, both manual and electronic;

- there are documented procedures for booking health records out from the normal filing system which enable rapid retrieval of health records and prevent misfiles;

- tracer and tracking systems facilitate timeous retrieval of health records;

- there is a documented procedure for splitting fat folders including cross-referencing of the volumes such that clinical staff may efficiently use them. Closed volumes are suitably labelled;

- there is a documented procedure relating to the return of patient held records to the health records department when the episode of care for an individual patient is complete;

- contents of the health record are filed in the correct order according to the design of the health record folder and dividers. Documents are securely fastened within the folder;

- the responsibility for filing of loose documentation is clearly defined;

- there is a system to ensure that staff routinely remove poorly filed and torn health records to reassemble or re-cover;

- there are documented procedures for the transportation of health records within and outwith health board boundaries;

- there are documented procedures for handling subject access and other legal requests with clear responsibility for responding by fully trained dedicated staff who process requests efficiently and in accordance with the law;

- there is a mechanism to help identify any misfiled health records, e.g. colour coding;

- there are documented procedures for the retention, archiving or destruction of health records in accordance with national guidelines. The method of destruction must ensure that confidentiality is maintained at all times;

- there is a set of performance indicators which demonstrate the efficiency of health records management. These should monitor such things as health record availability, use of temporary folders and timescales for receipt of health records at wards following emergency admission.

1.5.4. Archiving and Disposal of Health Records

There is a documented procedure for the retention, destruction or archiving of health records. See Annex D of the Scottish Government Records Management NHS Code of Practice (Scotland). The method of destruction must ensure that confidentiality is maintained at all times. The procedure specifies the timescale for retention for all types of health records and media and the procedure for transfer between media.

1.6. Legal and Professional Obligations

All NHS health records are public records under the Public Records (Scotland) Act. The Board will take actions as necessary to comply with legal and professional obligations such as:

- he Data Protection Act 1998;

- The Common Law Duty of Confidentiality; and

- The NHS Scotland Confidentiality Code of Practice;

- Access to Health Records Act 1990;

and any new legislation affecting health records management as it arises.

1.7. Roles and Responsibilities

1.7.1. Data Controller

The Chief Executive Officer has overall accountability for ensuring that health records management operates correctly/legally within the Board. The Chief Executive Officer may delegate responsibility for management and organisation of health records services to the Chief Operating Executive who is responsible for ensuring appropriate mechanisms are in place to support service delivery and continuity. Health records management is key to this, as it will ensure appropriate and accurate information is available as required.

1.7.2. Caldicott Guardian

The Boards' Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. The Caldicott Guardian has responsibility for:

- ensuring the Board is fulfilling all legal obligations in managing patients' health records;
- agreeing and reviewing internal protocols governing the protection and use of patient identifiable information by Board staff;
- agreeing and reviewing protocols governing the disclosure of patient information across organisational boundaries, e.g. with social services and other partner organisations, contributing to the local provision of care;
- developing the Board's security and confidentiality policies;
- representing confidentiality requirements and issues to the Board, advising on annual improvement plans and agreeing and presenting annual outcome reports.

1.7.3. Records Management/Information Governance Steering Group

The Boards' Health Records Management/Information Governance Steering Group/Committee is responsible for ensuring that the Health Records Management Policy is implemented through endorsement of the Health Records Management Strategy.

1.7.4. Designated Officer

The designated officer (Head of Health Records Services/Health Records Manager) holds a health records qualification or is suitably trained in health records practices. This officer has professional responsibility for the overall development and maintenance of health records management practices throughout the Board and for ensuring that related policies and procedures conform to the latest legislation and standards on data protection, patient confidentiality and health records practice. This officer is also accountable for the release of all patient clinical information for data subject access and medico-legal purposes.

1.7.5. Staff Responsibility for Record Keeping

All NHS employees are responsible for any health records which they create or use. This responsibility is established and defined by the law (Public Records (Scotland) Act 1937).

Furthermore as an employee of the NHS, any health records created by an employee are public records.

All Board staff whether clinical or administrative, who create, receive and use health records have records management responsibilities. All staff must ensure that they keep appropriate records of their work and manage those health records in keeping with this policy and with any guidance subsequently produced.

Everyone working for or within the NHS who records, handles, stores or otherwise comes across patient information has a personal common law duty of confidence to patients and to his or her employer. The duty of confidence continues even after the death of the patient or after the employee or contractor has left the NHS.

Breach of this policy will mean the organisation is not safeguarding information entrusted to it, which in some circumstances may render the organisation liable to prosecution. It is therefore essential that staff within the organisation with responsibility for records management comply with the policy otherwise they may be subject to disciplinary procedures.

1.8. Retention and Disposal Schedules

It is a fundamental requirement that all of the Boards' health records are maintained for a minimum period of time for clinical, legal, operational, research and safety reasons. The length of time for retaining health records will depend on the record type.

The Health Board has adopted the minimum retention periods set out in Annex D of the overarching Code of Practice. The locally agreed retention schedule can be found at (A2). The local retention schedule will be reviewed every 3 years or earlier in the light of legislative or Scottish Government changes.

1.9. Health Records Inventory

The Health Board requires knowing what records are held, where they are kept and how the information contained within the records is being used. An up to date health records inventory will be maintained by the Head of Health Records Services/Health Records Manager. This will identify all record collections/information sets that exist within the organisation, the volume of records, the type of media on which they are held, their physical condition, their location, the physical and environmental conditions in which they are stored and the responsible manager. The Head of Health Records Services /Health Records Manager should be made aware when new collections of records or information sets are created or where management arrangements or physical locations change. A sample records inventory survey form can be found at (A3).

1.10. Health Records Management Systems Audit

The Health Board will regularly audit the records management practices for compliance with this policy. Auditing health records policies and procedures will be done on a systematic basis. The audit will compare current operational practice against defined procedures. The audit cycle will include self assessment against the Information Governance, Quality Improvement Scotland and Patient Records and Information Management Accreditation Programme Standards (if the organisation subscribes to the accreditation and development of health records programme). (A

summary of these standards can be found at A4.)

Audit Cycle:

1.11. Health Records Management Improvement Plan

The Health Board has formulated an Improvement Plan identifying programmed activity for delivery of the Health Records Strategy. This identifies tasks related to each of the development areas with achievable milestones and timescales for implementation. Progress will be monitored through audit and compliance with the Information Governance and Patient Records and Information Management Accreditation Programme standards (if the organisation subscribes to the accreditation and development of health records programme). The Improvement Plan can be found at (A5).

1.12. Health Records Policies and Procedures

The Head of Health Records Services/Health Records Manager is responsible for planning and documenting Health Records departmental policies and procedures thus providing standardisation of work tasks throughout the department. In this context a procedure is a structured, action orientated list of sequential steps involved in carrying out a specific job. It is a series of related steps designed to accomplish a specific task. All Health Records Departments should have a policy and procedure manual to ensure that all staff members are undertaking their duties in a consistent way. Health records policies and procedures associated with this document can be found at A6.

1.13. Training

All staff employed by the Health Board including volunteers and contractors are given training on their personal responsibilities for health records keeping. This includes the creation, use, storage, security and confidentiality of health records. Appropriate training should be provided for all users of the health records systems to meet local and national standards. All new employees to the organisation will be given basic training as part of the organisation's induction process. Additional training in the specifics of health records management will be provided where appropriate. Training is tailored to specific staff groups and functions including the following:

- all current relevant legislation and NHS standards;
- all current relevant organisation policies and procedures;
- caldicott requirements;

- patient confidentiality and the security of records, whether paper or electronic;
- Data Protection Act 1998;
- Access to Health Records Act 1990;
- Scottish Government Records Management NHS Code of Practice (Scotland);
- secure destruction of confidential waste;
- individuals rights to access information (Data Protection Act 1998/ Mental Health (Scotland) Act 2003);
- NHS Scotland Code of Practice on Confidentiality;
- Patient Records and Information Management Accreditation Programme (PRIMAP).

Health records practitioners and personnel are pivotal to the management of health records systems and should receive customised training in health records practice. The policy and procedure manual is a key management tool and should form the basis for all health record system specific training.

The Scottish Health Records Forum acknowledges the effort of the sub group in drafting this policy for use across NHS Scotland. It is hoped the document will provide a framework which can be customised for use at individual NHS Board level.

Mr Robert H Bryden, NHS Ayrshire & Arran (Chair)
Miss May McConnell, NHS Ayrshire & Arran
Mrs Marilyn Horne, NHS Glasgow & Clyde
Ms Debbie Baird, NHS Ayrshire & Arran
Mrs Anne Allison, NHS Ayrshire & Arran
Mrs Margaret Kerr, NHS Ayrshire & Arran
Ms Fiona Crawford, NHS Ayrshire & Arran
Ms Fiona Hutchison, NHS Forth Valley

2. DEFINITIONS & ACRONYMS

2.1. Definitions

Health Record	Also referred to as: • Medical record • Case note • Case record • Patient record
Policy	Strategy / plan / guidance / principal / course of action.
PRIMAP	The Healthcare Accreditation and Quality Unit (CHKS Limited) administer a patient records and information management accreditation programme. This is a standards based programme of organisational development and support to health records departments in UK Acute Trusts and has recently extended its remit to cover primary care organisations. PRIMAP is a nationally recognised programme based on peer review methodology and has been mandated across Wales for Acute and Community Hospital Trusts. NHS Ayrshire & Arran, Lothian and Tayside currently subscribe to the programme. In addition PRIMAP has undertaken clinical coding audits. NHS organisations wishing to participate in the programme pay an annual subscription which entitles them to access the standards and to participate in development days. Typically the health records service will spend 6 – 18 months working with the standards before the survey by an external team of healthcare accreditation and quality unit surveyors takes place. CHKS Accreditation will be awarded to those organisations that have demonstrated compliance with the standards.
Procedure	A structured, action orientated list of sequential steps involved in carrying out a specific job. It is a series of related steps designed to accomplish a specific task.

2.2. Acronyms

CHI	Community Health Index
CTG	
ECG	Electrocardiogram
HDL	Health Department Letter
IG	Information Governance
PRIMAP	Patient Records and Information Management Accreditation

2.3. References

Access to Health Records Act 1990:
http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900023_en_1.htm

Data Protection Act 1998:
http://www.sehd.scot.nhs.uk/mels/2000_17.doc

The Management Retention and Disposal of Personal Health Records

Human Rights Act 2000

Information Governance Standards:
http://www.elib.scot.nhs.uk

Medical Reports Act 1988:
http://www.opsi.gov.uk/ACTS/acts1988/Ukpga_19880028_en_1.htm

National eHealth Strategy:
http://www.ehealth.scot.nhs.uk

PRIMAP (Patient Records and Information Management Accreditation Programme)
www.chks.co.uk

Public Records (Scotland) Act 1937:
http://www.nas.gov.uk/recordKeeping/publicRecordsScotlandAct1937.asp

Quality Improvement Scotland - Standards for Record Keeping:
http://www.nhshealthquality.org/nhsqis/files/CGRM_CSF_Oct05.pdf

The Computer Misuse Act 1990:
http://www.opsi.gov.uk/ACTS/acts1990/Ukpga_19900018_en_2.htm

A2 - LOCAL RETENTION SCHEDULE FOR HEALTH RECORDS AND DATASETS

If there are local retention schedules which accord to this Code of Practice, attach these to printed out versions of this document.

A3 - SAMPLE HEALTH RECORDS INVENTORY SURVEY FORM

1 FORM TO BE USED FOR EACH RECORD COLLECTION

RETURN DATE: _____

MANUAL RECORDS INVENTORY FORM			
Directorate		Location	
Department/Service			
Contact Name		Telephone No:	

1.	Do you store manual records in the department?	Yes ☐ If yes, please complete and return the questionnaire No ☐ If no, please return the questionnaire
2.	Name of the record	
3.	Alternative name of the record (where appropriate)	
4.	Are duplicates of the record held?	Yes ☐ If yes, where? No ☐
5.	Who is responsible for managing the record?	Name : _____ Job Title: _____ Tel No: _____
6.	Format of the record	Paper ☐ Film / X-ray ☐ Microform ☐ Other (specify) _____
7.	Description of the record	
8.	Why do you create/collect this information?	Patient care/admin ☐ Research ☐ Clinical audit ☐ Other _____ Central returns ☐ _____ Business/corporate ☐
9.	Where does the information come from?	Generated within the department ☐ Transferred from within the organisation ☐ Transferred from outside the organisation ☐
10.	Does the record contain personal data?	Yes ☐ No ☐ If yes, is it identifiable? Yes ☐ No ☐
11.	Is access to the record, or information it contains, restricted within the directorate?	Yes ☐ No ☐ If yes, with who is it shared? Does it include access to personal data? Yes ☐ No ☐ Why is it shared?

12.	Is the record, or information it contains, shared with other members of staff <u>within the organisation?</u>	Yes ☐ No ☐ If yes, with whom is it shared? Does it include access to personal data? Yes☐ No ☐ Why is it shared?
13.	Is the record, or information it contains, shared with others from <u>outwith the organisation</u>?	Yes ☐ No ☐ If yes, with whom is it shared? Does it include access to personal data? Yes☐ No ☐ Why is it shared?
14.	How many records are held? (estimate)	Total _____ Active _____ (if known) Inactive _____ (if known)
15.	Is there a register, index etc of the records?	Yes ☐ If yes, where is it held? No ☐
16.	Where are the records stored?	(e.g. nurses office – etc)
17.	Is there currently sufficient storage available?	Yes ☐ No ☐
18.	Will sufficient storage be available in the future?	Yes ☐ No ☐ If yes, for how long 6 months ☐ 1 year ☐ 2 years ☐ Other _____

19.	Are these locations secure? (e.g. locked cabinets, locked rooms, stores etc)	All ☐ Comments Most ☐ Half ☐ Few ☐ None ☐	
20.	Are any of the stores:	Shared with cleaner, other departments etc ☐ Outside building (e.g. garage, portacabin etc) ☐ Structurally unsound ☐ Evidence of damp, dry rot, pests etc ☐ Inadequate lighting ☐ Inappropriate/insufficient shelving ☐ Dirty/messy ☐ Unsafe to work in ☐ Other concerns: _____	
21.	Do you have a record tracking system should records leave the department?	Yes ☐ If yes, is it Paper based ☐ No ☐ Electronic ☐	
22.	Is there a business continuity plan for the records?	Yes ☐ If yes, specify No ☐ Don't know ☐	
23.	Have you identified how long the records must be kept?	Yes ☐ No ☐	
24.	What action is taken when the retention period is exceeded?	Destroyed ☐	How
		No action taken ☐	Why?
		Archived elsewhere ☐	Where?
		Other ☐	Specify

FURTHER COMMENTS

If you have any further comments or questions regarding the information you hold (e.g. creation, maintenance, storage, retention, disposal etc) please specify below.

PLEASE RETURN TO:
_____

A4 - INFORMATION GOVERNANCE STANDARDS 3E.2 : PATIENT RECORDS

IG Reference	Standard	Cross referred to PRIMAP Standard	Standard	Reference in this report
5.001	The Board has an approved patient records policy, which includes storage to accommodate casenotes etc.	Standard 1.1 Standard 1.2	There is a dated, documented organisation-wide health records management strategy approved by the Board, or its delegated Committee. This has been written/reviewed within the last three years. The relevant staff are aware of the strategy and there is evidence of implementation. There is a dated, documented health records management programme or action plan that identifies prioritised activity to support the implementation of the records management strategy. This has been written/reviewed within the last three years. The relevant staff are aware of the programme action plan and there is evidence of implementation.	5.2.8 5.2.9 5.3.1

IG Reference	Standard	Cross referred to PRIMAP Standard	Standard	Reference in this report
5.002	There is a clearly identified, suitably qualified and supported lead individual responsible for patient records.	Standard 1.5 Standard 1.6 Standard 1.8	There is a manager with professional accountability for the health records service whose job description is consistent with the aims and objectives of the service. Board level responsibility for health records management is clearly defined and there are clear lines of professional accountability for health records management and systems throughout the organization. The health records service is managed by a qualified person.	7.4

IG Reference	Standard	Cross referred to PRIMAP Standard	Standard	Reference in this report
5.003	The Board has a Patient Records Committee, which makes decisions on policy matters and which includes representation from clinical and non-clinical staff and is linked appropriately to other Information Governance groups.	Standard 8.1 Standard 8.2	There is a designated body (i.e. Health Records Committee or equivalent), with documented terms of reference. Minutes of meetings are kept. The designated body has multi disciplinary representation. This includes representatives from the various groups that make entries in the health records, (e.g. clinical professionals), as well as representatives of the administrative staff that deal with records (e.g. managers and operational staff)	7.3

IG Reference	Standard	Cross referred to PRIMAP Standard	Standard	Reference in this report
5.004	The Board ensures that the environment and office storage areas complies with all current, relevant Health and Safety legislation and fire regulations	Standard 2.1 Standard 2.2	Health records storage areas and associated office conform to all current relevant legislation and guidance regarding health and safety including the Health and Safety at Work Act 1974, Workplace (Health, Safety & Welfare) Regulations 1992, Health & Safety (First Aid) Regulations 1981, Health & Safety (Display Screen Equipment) regulations 1992, Manual Handling Operations Regulations 1992 and Fire Regulations Regular risk assessments are undertaken, in line with the organisation's Risk Management Strategy for all staff and areas within the Health Records service.	5.2.1 5.2.2 5.2.3 5.2.4 5.2.5 5.2.6

IG Reference	Standard	Cross referred to PRIMAP Standard	Standard	Reference in this report
5.005	The Board has mechanisms in place to ensure that all health records managers and staff receive training in health records.	Standard 7.1	All personnel working within the Health Records service have an induction training programme provided on appointment to the organisation.	13
5.006	All scanned documents meet legal admissibility standards prior to the destruction of the paper record.	Standard 3.1.9	There are dated, documented procedures for the management of electronic records and for safeguarding data held on computer systems by the organisation. These have been written/reviewed within the last 3 years. The relevant staff are aware of the procedures and there is evidence of implementation	5.3.13 5.4
5.007	The Board ensures that the Community Health Index (CHI) number is used on all communications concerning individual patients, including requests, reports and letters.	Standard 3.2.1	The organisation uses the NHS number as the patient identifier (CHI in Scotland).	5.1.2

A5 - HEALTH RECORDS MANAGEMENT IMPROVEMENT PLAN

Strategic Aim/ Improvement	Action	Reference to Relevant National Standards	Progress	Responsible Person	Timescale
Records Management organisation/system					
eHealth strategic aim /improvement (if applicable)					
Record creation					
Record keeping					
Record storage and retention					
Records management					
Records inventory					
Records audit					
Training					
Accountability					
Monitoring and review					

Sample Action from Health Records Management Improvement Plan

Strategic Aim/ Improvement	Action	Reference to Relevant National Standards	Progress	Responsible Person	Timescale
Records Management					
Improve the availability of health records in clinics and ward areas	• Regular monitoring of case record availability • Ensuring that standards for the safe transport of case records are adhered to • Monitoring of tracering systems • Resolving issues associated with lack of access to IT systems • Addressing portering and transport problems across the Board			Health Records Manager Health Records Supervisors Health Records Manager Head of Health Records Services /eHealth Services Manager Portering Services Manager	

A6 - HEALTH RECORDS POLICIES & PROCEDURES POLICES & PROCEDURES

There is a policy for the retention, destruction or archiving of health records in accordance with national guidelines. The method of destruction must ensure that confidentiality is maintained at all times.	001	PRIMAP Standard 4 (Point 4.9)	
There is a policy on confidentiality and the release and management of information that complies with the relevant legislation and national guidance. The policy sets out how the organisation ensures that information held about patients, their families and staff is managed confidentially.	002	PRIMAP Standard 4 (Point 4.17)	IG Standard 6.005
There is a policy for ensuring the physical security of areas where health records may be accessed e.g. locking doors; filing cabinets etc.	003	PRIMAP Standard 4 (Point 4.21)	
There is a policy in respect of safe and secure transportation of health records within and without the organisation's boundaries.	004	PRIMAP Standard 4 (Point 4.28)	IG Standard 5.001
There is a policy in respect of receipt and transmission of faxes and electronic data flows containing confidential patient-identifiable information.	005	PRIMAP Standard 4 (Point 4.31)	
There is a policy for the creation and subsequent incorporation of temporary records.	006	PRIMAP Standard 4 (Point 4.38)	
There is a protocol for safe manual and object handling practices that all staff are fully aware of.		PRIMAP Standard 2 (Point 2.11)	Refer to NHS Boards' Moving and Handling Procedures
There is a mechanism to ensure that all equipment used in the department conforms to the appropriate legislation.		PRIMAP Standard 2 (Point 2.14)	Refer to NHS Boards' Estates Procedure for Equipment checks
There are procedures for the safe storage and retrieval of health	007	PRIMAP Standard 2 (Point	

records, both manual and electronic.		2.27)	
There are procedures for booking records out from the normal filing system, which enables rapid retrieval of records and prevents misfiling.	008 009	PRIMAP Standard 2 (Point 2.28)	
There is a method for indicating alert to risk factors, which is used consistently in all patient records, with the case note containing a designated place for healthcare professionals to record actual allergies/risks; to be signed and dated.	010	PRIMAP Standard 3 (Point 3.4) *Please note policy 010 has not been drafted as it was felt this would be best developed at local hospital or NHS Board level.*	
There is a procedure for splitting fat folders, including cross-referencing of the volumes, such that clinical staff may efficiently use them.	011	PRIMAP Standard 3 (Point 3.10)	
There is a procedure relating to the return of patient-held records to the health records department when the episode of care for an individual patient is complete.	012	PRIMAP Standard 3 (Point 3.11) *Please note policy 010 has not been drafted as it was felt this would be best developed at local hospital or NHS Board level.*	
There is a procedure for issuing local patient identifiers. The relevant staff are aware of the procedure and there is evidence of implementation.	013	PRIMAP Standard 4 (Point 4.10)	
There is a procedure for updating patient demographic details (e.g. change of address) when these are notified to a member of the organisation's staff.	013	PRIMAP Standard 4 (Point 4.12	
There is a procedure for handling subject access requests, with clear responsibility for responding by fully trained and resourced staff who process such requests efficiently and in accordance with	014	PRIMAP Standard 4 (Point 4.18) *Please note policy 010 has not been*	

the law.		*drafted as it was felt this would be best developed at local hospital or NHS Board level.*	
There is a procedure in place which identifies the responsibility for filing of loose documentation within case records. This makes reference to the responsibility of all stakeholders.	015	PRIMAP Standard 3 (Point 3.15)	

001. Retention, Destruction and Archiving Of Health Records

1. Opening Statement

The data protection act 1998 sets out a series of standards which NHS Boards and other NHS Bodies must meet in order to comply with the law. One of these is that they must comply with the Fifth Data Protection Principle which is that "Personal Data processed for any purposes shall not be kept for longer than is necessary for that purpose or those purposes".

2. Retention Periods

Legal requirement is (x) years but local policies may differ.

List local retention periods for deceased, current, non current health records etc.

3. Exceptions

List categories that must not be destroyed e.g. pre 1948 etc.

4. Process

List your local procedure for:

Identification of records suitable for destruction

Recording date of destruction

Confidential destruction/ disposal of health record

Definition of Terms & Acronyms

Reference (National/local guidelines, standards and legislation)

Links (related policies and guidance) can also include web links if applicable

HDL(2006)28 : The Management, Retention and Disposal of Administrative Records
http://www.sehd.scot.nhs.uk/mels/HDL200628.pdf

NHS MEL (2000)17 : Data Protection Act 1998
www.sehd.scot.nhs.uk/mels/200017.doc

The Management Retention and Disposal of Personal Health Records (currently in draft)

Policy 007 : Medical Records Filing System

002. Confidentiality/Security and the Release and Management of Information

1. Opening Statement

Everyone working in the NHS has a legal obligation to keep all patient related information confidential.

Security and Confidentiality of data applies not only to manual health records but also computer systems both administrative and clinical, e.g. PAS, Laboratory, Radiology systems etc.

2. Your Responsibility

Staff should read and be aware of the content of the NHS Code of Practice on protecting patient confidentiality (yellow booklet). This should be provided with letter of appointment.

All staff must sign a confidentiality statement on commencement of duty.
Any breach of confidentiality will attract disciplinary action, which may lead to dismissal.

3. What Constitutes Confidential Data

All information held about a patient is regarded as confidential. This includes: demographic/administrative data as well as clinical data, e.g. name, address, postcode, telephone number, clinic attended, appointment details.

Give examples of what constitutes confidential data and how confidentiality may be breached.

4. Security

Describe physical controls e.g.

ID badges, restricted access, key pads etc

5. Security of Computerised Data

Describe system controls e.g.

Passwords/unique user name, level of access, private and unintelligible to others, audit trails ,follow up action, termination of employment, secure areas, logging off etc.

6. Staff Members with a Legitimate Right to Access Confidential Data

Medical, Nursing, Research, Health Records, Medico/legal, clinical effectiveness, Allied Health Care Professionals etc.

7. Data Protection Act/Access to Health Records Act

Refer to Data Protection Act 1998 and Access to Health Records Act 1990.

Describe on a step by step basis the process for receipt of data subject access requests, processing and release.

Timescale, Mandates.

List all forms of access.

8. Information Sharing

This process usually requires the consent of the patient. This may be implicit i.e. implied when the patient seeks medical care or explicit i.e. the patient makes an informed decision to consent to the release/sharing of their data.

Examples of information which may be divulged under statutory obligation include:

List :

Notification of Infectious Diseases
Notification under child protection arrangements, DSS BR409 etc.

Definition of Terms & Acronyms

Reference (National/local guidelines, standards and legislation)

Links (related policies and guidance) can also include web links if applicable

Data Protection Act 1998 www.sehd.scot.nhs.uk/mels/2000_17.doc

Access to Health Records Act 1990

Caldicott Principles
www.confidentiality.scot.nhs.uk/caldicott.htm
www.elib.scot.nhs.uk

"Protecting Personal Health Information" – Information Guide for Patients
(Produced by ISD)

"Confidentiality – It's Your Right"
(Produced by NHS Scotland)

"Confidentiality – A guide for young people under 16" (Produced by NHS Scotland)

"How to see Your Health Records"
(produced by NHS Scotland)

Policy: Local IT Security

Health Rights Information Scotland (HRIS)
http://www.hris.org.uk

003. Security of Health Records Storage Areas

1. Opening Statement

Storage has a huge impact on the effectiveness of the service we provide. Areas must be secure to protect records against loss, damage or access by unauthorised persons.

2. Health Records Libraries

List local controls procedures i.e. security – key pad, swipe card etc.

3. Peripheral Office Accommodation and Storage Areas

List local physical controls and procedure for access (including out of hours access).

4. Off-site Storage

Include details: off-site storage location and supplier and out of hours access.

5. Electronic Storage

Levels of access e.g. electronic document management system.

6. Access

List staff groups who are allowed to access the various storage areas.

Definition of Terms & Acronyms

Reference (National/local guidelines, standards and legislation)

Links (related policies and guidance) can also include web links if applicable

Policy 002 : Confidentiality/Security and the Release and Management of Information

Local Moving and Handling, Health & Safety, Security and Lone Working policies

004. Transportation of Health Records Within and Outwith Organisation Boundaries

1. Opening Statement

Patients' Health Records contain personal and sensitive information and are highly confidential documents. Care must be taken when transporting them within or outwith the hospital.

2. Transportation of Health Records within Hospital

Local procedure for transporting to clinics/secretarial staff and wards. Use of trolleys. Local procedure for porter delivery.

3. Transportation of Health Records to other Hospitals within the Health Board Area

Physical controls e.g. Sealed boxes. Dedicated portering service if applicable.

4. Transportation of Original or Copy Health Records to Hospitals or Authorised Agencies outwith the Internal Mail Delivery Service

Physical controls e.g.

Recorded Delivery, Taxi, sealed boxes, double envelopes etc.

Photocopy sent to reduce risk of losing original etc.

5. Lifting and Handling of Health Records

Proper use of trolleys, keep bundles manageable, See manual handling policy

6. Staff Transportation of Health Records

Staff awareness of procedures for safe and confidential physical transportation of health records throughout the organisation.

Definition of Terms & Acronyms

Reference (National/local guidelines, standards and legislation)

Links (related policies and guidance) can also include web links if applicable

Policy 002 : Confidentiality/Security and the Release and Management of Information

Policy 008 : Case record Tracking / Tracering

005. Electronic Transmission of Patient Identifiable Data

1. Opening Statement

The protocol should conform with the guidance contained within NHS MEL (1997) 45 “Guidance on the use of facsimile transmissions for the transfer of personal health information” and local policy on e-mailing patient identifiable data.

For the safe transmission of electronic patient data no information identifying the patient should be faxed.

2. Safe Haven

Record location of safe haven fax.

3. Removal of Demographic Details

List steps followed before faxing information i.e. photocopy original, blank out patient identifiable information etc.

4. Receipt of faxes

Acknowledge receipt, date stamp etc.

5. Receipt of Electronic Referrals

Detail local procedure on receipt of electronic referrals etc.

Definition of Terms & Acronyms

Reference (National/local guidelines, standards and legislation)

Links (related policies and guidance) can also include web links if applicable

NHS MEL (1997)45 “Guidance on the use of facsimile transmissions for the transfer of personal health information”

Policy 002 : Confidentiality/Security and the Release and Management of Information

Policy 009 : Missing Case records

006. Temporary And Duplicate Case records

1. Opening Statement

A temporary case record folder may only be issued on the instruction of a member of the management team when she/he is satisfied that an exhaustive search has been carried out and original case record cannot be found.

When duplicate registrations are identified action must be taken to amalgamate both physical case record and computerised system.

2. Procedure for Issuing Temporary Case record Folder

List your local procedure which explains step by step guide i.e. inform clinician, obtain copies of documentation, creating a temporary folder etc.

3. Amalgamation of Documentation

Actions taken when original case record found i.e. shredding of copy documents etc.

4. Tracking of Temporary Case records

Local policy i.e. recording electronically and manually.

5. Amalgamation of Duplicate Registrations/Case records

Local procedure i.e. merge patient index record and contents of both case records physically amalgamated into correct folder etc.

Definition of Terms & Acronyms

Reference (National/local guidelines, standards and legislation)

Links (related policies and guidance) can also include web links if applicable

Policy 009: Missing Case records

007. Medical Records Filing Systems

1. Opening Statement

The prime purpose of a Health Records Department is to bring together 3 key players – the patient, the doctor / healthcare professional and the case record i.e. have the right case records in the right place at the right time.

Whichever filing system is used, it is imperative that case records are filed accurately as a great deal of time can be wasted searching for mis-filed records.

Failure to produce the case record can result in:

- past medical history being unavailable;
- refusal/delay by Consultant to see patient;
- cancellation of procedure;
- distress to patient/relative;
- increase in clinical risk.

2. Filing System

Describe local filing procedure for each records collection, e.g. terminal digit, alphabetical etc.

3. Case records Storage Systems

Describe the various storage systems in use throughout the Board including secondary storage/off-site storage and other media.

4. Electronic Patient Records

Describe local procedures for accessing /indexing documentation and retrieval of records.

Definition of Terms & Acronyms

Reference (National/local guidelines, standards and legislation)

Links (related policies and guidance) can also include web links if applicable

Policy 008: Case record Tracking / Tracering

Policy 002: Confidentiality/Security and the Release and Management of Information

Policy 001: Retention, Destruction and Archiving of Health Records

Local Moving & Handling policy

008. Case record Tracking / Tracering

1. Opening Statement

When case records are removed from the filing system or given from one person to another the chart tracking system is updated. Failure to update the chart tracking system as case records are removed from file or change location may result in case records not being available when required.

2. General Principle

Describe general principle for updating the chart tracking system including the accountability for each staff group in the patient process. E.g. Health records, ward clerks, medical secretaries etc.

3. Process for Confirming Case records Back into Current File

Local procedure i.e. medical records staff only re filing into current filing area

4. Computer System Downtime

Describe local procedures which are put into place i.e. manual tracers, registers etc

Definition of Terms & Acronyms

Reference (National/local guidelines, standards and legislation)

Links (related policies and guidance) can also include web links if applicable

Policy 007 : Medical Records Filing Systems

Policy 004 : Transportation of Health Records within and outwith Organisation Boundaries

009. Missing Case records

1. Opening Statement

Health Records staff are responsible for ensuring that all patients' case records are available for any attendance or admission the patient may have at hospital. In addition to this, case records require to be obtained timeously for a number of administrative processes.

2. Chart Tracking History

Describe steps taken to obtain history, e.g. checking last and previous locations chart tracking system.

3. Procedure for Obtaining Missing Case records

List steps i.e. search shelves, clinic bundles (not tracked), secretaries offices etc.

4. Escalating Problem if Case records Cannot be Found

Local procedure e.g.. passed to Supervisor, Issue of Temporary Folder.

5. Case record Located

Local procedure i.e. original documentation amalgamated, copies shredded, update tracking system.

Definition of Terms & Acronyms

Reference (National/local guidelines, standards and legislation)

Links (related policies and guidance) can also include web links if applicable

POLICY 006: Temporary and Duplicate Case records

011. Splitting of Voluminous Case record Folders

1. Opening Statement

When the documentation relating to a patient can no longer be securely filed in one volume, a second volume is created to hold the overflow. Some patients may require a third or fourth volume in order to keep the notes manageable.

2. Numbering

Outline your local procedure for numbering each volume.

3. Procedure for Splitting Case records

List contents of each volume.
Culling and Retention Procedure.
Outline your local Tracking procedure.
Describe process for labelling closed records.

Definition of Terms & Acronyms

Reference (National/local guidelines, standards and legislation)

Links (related policies and guidance) can also include web links if applicable

Policy 007 : Medical Records Filing Systems

Policy 008: Case record Tracking / Tracering

Policy 001: Retention, Destruction and archiving of Health Records

013. Searching and Updating Patient Demographic Data In The Master Patient Index

1. Opening Statement

The Master Patient Index is an alphabetical key to records which are filed numerically. It allows patient search, amendment to patient demographics and registration of new patients creating a departmental patient identification number which is linked to the Community Health Index number as the unique patient identifier. It can be kept on a computerised patient administration system or on a manual card system.

2. Information Held on Master Patient Index

List demographic data held on MPI, e.g. date of birth, name, post code, CHI number, GP etc.

3. Search and Registration Techniques

Describe local search procedures e.g.:

- full patient demographics, surname, forename, date of birth, name, sex, CHI etc;
- DOB only;
- homonyms / alias;
- combination of patient demographics, e.g. surname and postcode or name and CHI etc.

4. Maintenance of Master Patient Index

Describe procedures for updating the Master Patient Index, e.g. change of patient demographic details, recording deaths etc.

5. Unknown Patients

Describe procedures for registration of unknown patients.

6. Data Quality

List mandatory fields
Process for duplicate checking
Process for notification of duplicates
Accountable officer

Definition of Terms & Acronyms

Reference (National/local guidelines, standards and legislation)

Links (related policies and guidance) can also include web links if applicable

015. Filing of Loose Documentation

1. Opening Statement

During the course of a patients' treatment within the hospital, many documents and reports are produced by the various clinical and laboratory departments concerned with the patients' care. These documents and reports arrive at a variety of destinations within the hospital. Health Records, ward clerks and medical secretarial staff are responsible for ensuring loose documentation is timeously and correctly filed within the Health Record folder.

2. Health Records Department

Describe procedures and accountability for loose documentation

3. Medical Secretarial Level

Describe procedures and accountability for loose documentation

4. Ward Level

Describe procedures and accountability for loose documentation

5. Accident and Emergency

Describe procedures and accountability for loose documentation

Definition of Terms & Acronyms

Reference (National/local guidelines, standards and legislation)

Links (related policies and guidance) can also include web links if applicable

ANNEX F – NHSSCOTLAND PERSONAL HEALTH RECORDS MANAGEMENT STRATEGY FOR NHS BOARDS

Please note *- this annex was developed by a subgroup of The Health Records Forum, and has been the subject of a recent consultation. It has been included in this overarching Code of Practice to provide further advice and support to NHS Boards in the development of their local health record strategy. It is recognised by the Scottish Government eHealth directorate as a useful tool for Boards in helping them meet their records management obligations.*

1. Introduction

This document directs the principles and practice for managing health records at the Health Board. The organisation uses a hybrid of computer and paper records to support patient processes. This strategy sets out how all patient records will be managed and replaces and supersedes any previous health records management strategies.

Health records management falls within the remit of the health records service. The aim of the health records service is to ensure that procedures are in place to bring together the health professional and accurate, relevant patient information/documentation at the correct time and place to support patient care. The service comprises of 6 main elements:

- control and maintenance of patient appointment systems;
- initiation, retention, safekeeping and production of patients' records;
- registration and recording of all patient encounters;
- compilation, validation and submission of all Scottish Morbidity Records and statistical returns;
- provision of an administrative service to respond to medico-legal and data requests made under the relevant "Acts";
- provision of clerical, administrative and reception services to support clinicians in the delivery of clinical care.

Records management is a key component of the health records service.

The strategy details the aims, aspirations and targets of what we aim to achieve with our health records management programmes. It provides direction for what we want to achieve within the organisation and also defines what resources are required in future to deliver effective records management programmes.

Records management is the field of management responsible for the efficient and systematic control of the creation, storage, retrieval, maintenance, use and disposal of health records, including processes for capturing and maintaining evidence.

Proper management of information and a strong records management programme requires adequate resources: sufficient funding, facilities, technologies and knowledgeable experienced people. Consideration of health records management principles requires timely inclusion into service objectives, plans and developments to ensure appropriate resource allocation and implementation of good practice.

The strategy is based on the requirements of the Scottish Government Records Management NHS Code of Practice (Scotland). This document covers management of all types of NHS health records throughout their lifecycle, from their creation and use to their final disposal.

This strategy also takes into account the recommendations and standards set by:

- Public Records (Scotland) Act 1937;
- Medical Reports Act 1988;
- The Computer Misuse Act 1990;
- Access to Health Records Act 1990;
- Data Protection Act 1998;
- Human Rights Act 2000;
- Quality Improvement Scotland – Standards for Record Keeping;
- Scottish Government Records Management NHS Code of Practice (Scotland);
- Scottish Government Health Department (Health Department Letters, Circulars and Policies);
- Patient Records and Information Management Accreditation Programme (PRIMAP);
- Information Governance Standards;
- National eHealth Strategy;
- ISD Data Definitions and Standards.

The strategy will be updated to include future developments such as new health records management guidance or changes in legislation as necessary.

The Health Records Management Strategy should be read in conjunction with the Health Records Management Policy.

2. Scope

2.1. This strategy relates to all clinical operational records held in any format by the Health Board as set out in The Management Retention and Disposal of Personal Health Records.

- within the strategy the terms 'Health Record', 'Patient Record' and ‘Case record’ are synonymous and includes:
  - records created and maintained by all health care professionals
  - records for all specialties
  - records for private patients treated on NHS premises

2.2. Health Records may be held in many formats, for example:

- paper records, reports, diaries and registers etc;
- electronic records;
- x-rays and other images;
- microform (i.e. microfiche and microfilm);
- audio and video tapes.

3. Aims

The aims of the Health Board Health Records Management Strategy is to ensure:

- a systematic and planned approach to health records management covering health records from creation to disposal;
- efficiency and best value through improvements in the quality and flow of information, and greater co-ordination of health records and storage systems;
- compliance with statutory requirements;
- awareness of the importance of health records management and the need for responsibility and accountability at all levels;
- appropriate archiving of non current health records.

4. Key Elements

The Health Records Management Strategy comprises the following key elements:

4.1. Responsibility and Accountability

The Chief Executive has overall accountability for ensuring that Health Records management operates correctly/legally within the Board. The Chief Executive may delegate responsibility for management and organisation of health records services to the Chief Operating Executive who is responsible for ensuring appropriate mechanisms are in place to support service delivery and continuity.

The Head of Health Records Services/Senior Health Records Manager has strategic and operational accountability for the creation, retrieval, storage, archiving and

disposal of all health records within the Board. The Board has in place a documented Health Records Management Policy and supporting documented procedures.

4.2. Quality

The Health Records Management Strategy aims to ensure that policies and procedures are in place to bring together the patient and health professional along with accurate, relevant reliable patient information and documentation at the correct time and place to support effective and safe patient care. The Health Records Management Policy and appendix of policies and procedures provides further detail concerning standards for the management of health records. Health records are managed in accordance with the recommendations and standards detailed in the introduction of this strategy.

4.3. Management

All health records are subject to the standards and legislation detailed at the Introduction of this document and the Board is responsible for ensuring that health records are managed accordingly. The Board has a detailed inventory providing details of the location and current status of all health record types. The Health Records Management Policy details procedures for the storage, retrieval, archiving and disposal of each record type. This procedure is in accordance with the minimum retention periods detailed in the Scottish Government Records Management NHS Code of Practice (Scotland). The Board is responsible for ensuring that adequate resources are made available to support effective records management, including making adequate provision for records growth and technological developments which enable records to be stored or transferred to other media.

4.4. Security

The Board provides systems which maintain appropriate confidentiality, security and integrity for all health records including their storage and use.

Health records in any form are highly confidential documents. The Board is responsible for ensuring that adequate physical controls are put in place to ensure the security and confidentiality of all patient identifiable information, whether held manually or computer. Policies and procedures can be found in the Boards Information Security Policy and local departmental procedures.

4.5. Access

Access to all patient identifiable information is on a strict need to know basis in accordance with the Caldicott principles, Data Protection Act 1998 , Information Governance Standards and various codes of professional conduct. Polices and procedures governing access to patient identifiable information are in accordance with these principles.

4.6. Legislation

Health records and associated clinical information are released to patients, their representatives and legal bodies in accordance with relevant and current legislation.

The Head of Health Records Services /Senior Health Records Manager is responsible for the processing and release of clinical information in accordance with documented procedures.

4.7. Audit

This Health Records Management Strategy will be audited on a bi-annual basis for compliance against the actions outlined within the Health Records Management Policy.

4.8. Training

As the volume and complexity of clinical information increases, we demand the highest standards of probity in the way it is gathered, recorded, stored and transmitted. These requirements are set out in the Introduction of this strategy.

In implementing the strategy, the Board will put in place training and guidance on legal and ethical responsibilities for all NHS staff involved with the creation, maintenance and ongoing management of health records. In addition to complying with legislation, this training will follow the HORUS principles :

- holding information securely and confidentially;
- obtaining information fairly and efficiently;
- recording information accurately and reliably;
- using information effectively and ethically;
- sharing information appropriately and lawfully.

Whenever possible nationally recognised training material which is referenced to appropriate publications will be used.

Ongoing workforce education plays a major part in preparing NHS staff to deliver effective, high quality services. There are numerous reasons for providing education and training in information handling, including maintenance and improvement of services, respect to patients as well as the need to comply with legislation in respect of data collection, storage and use. NHS Education for Scotland and NHS National Services Scotland (NSS) are working in partnership to develop a framework of educational support for Information Governance. Information Governance in NHS Scotland Planning for Workforce Education (currently in draft) will be a key tool to assist NHS Boards with the planning and implementation of local workforce development initiatives. This document will include an Information Governance competency framework describing the learning outcomes for each of the HORUS standards. Competencies will be grouped into levels Foundation, Intermediate 1, Intermediate 2 and Advanced in order that these can be applied to specific occupations, staff groups, professions etc.

4.9. Development Programme

All health records managers or those with a particular responsibility for the administration and management of health records will be able to access appropriate information and guidance concerning record keeping standards. Whenever possible national standards will be employed to manage all health records throughout the Board. A rolling programme of audit and performance indicators will be developed to enable assessment of individual records system against these standards. An improvement plan will be formulated taking cognisance of the development needs within each of the designated areas.

4.10. Improvement Plan

A documented health records management improvement plan that identifies prioritised activity to support the implementation of the Health Records Management Strategy can be found within (A5) of the Health Records Management Policy. This improvement plan identifies resources (human, financial and organisational) required to ensure that all NHS health records of all types are properly controlled, readily accessible and available for use when required and then eventually archived or disposed of in an appropriate way, regardless of the media on which they are held.

5. National Strategic Direction

'Partnership for Care' states:

"Our goal is to deliver an Integrated Care Record jointly managed by patients and professional NHS staff with in-built security of access governed by patient consent". In addition:

"integrated care records will take time to reach, but each step in their development will bring immediate benefits to patients, carers and health care professionals by enabling:

- service redesign and the shift in the balance of care provided in different settings;
- faster exchange of information between professionals;
- quicker efficient access to patient records for patients and health professionals (with built in patient confidentiality);
- continuous improvement through routine monitoring of quality standards set by external bodies.

The new Scottish Government are due to consult on the priorities for health and wellbeing and will announce their key objectives for the next few years.

Better Health, Better Care announced:

That a revised eHealth Strategy would be published in spring 2008. At time of writing the process of developing this strategy is underway, however the final

document following consultation has not yet been agreed by the eHealth Strategy Board. In the meantime there are several relevant sections in the former (draft) Strategy, and these are shown below.

The Electronic Health Record is an electronic and structured set of health information based around an individuals' health and care status and encounters across all healthcare sectors and settings. It is:

- brought together from diverse clinical settings with their individual electronic patient records via a single patient identifier – the Community Health Index (CHI) number;
- accessible from a wide variety of locations by the patient or care professional, given appropriate security and access rights;
- organised primarily to support continuing, efficient and quality care across the complete patient journey;
- protected by secure profiles which will ensure that access is on a 'need' basis and that the patient is aware of who can see what information;
- secure, with an audit trail of all individuals who have accessed the record and their interactions with it;
- added to both by health professionals and patients themselves;
- a replacement for existing paper records and used as a medico-legal record as well as a health record.

For the short to medium term the goal of EHR will not be achieved by a single all-encompassing software application. Such a product is not available on the market at this time. Our strategy, therefore, is founded on an iterative and incremental approach rather than 'rip and replace'. 'EHR' is an umbrella term used to describe all the clinical information about a patient which is held electronically and which can be brought together from the data repositories maintained by key software applications. EHR will be achieved through incrementally putting in place and connecting the necessary software and ICT infrastructure components.

Currently health records are mainly maintained as paper based documents, however with the progression of eHealth projects and electronic solutions the service will move to a hybrid model of paper based and electronic records both active and passive. Health records staff are critical to the successful delivery of these goals. The challenge of moving from manual to the vision of electronic integrated care records built on modern technology will require the application of the skills and experience of health records practitioners and personnel.

The National eHealth/IM&T Strategy further states:

"The single patient record is a holistic patient record that is accessible to those who require the information including patients and carers. Currently professional staff in

many settings hold fragments of the record, but none have access to the whole record".

The key elements of the eHealth high level plan for a single patient record endorse the move to one patient, one record jointly managed by patients and professional NHS staff with in-built security of access governed by patient consent. Reliable and consistent authentication of patient demographic information is vital when assembling different "fragments" into the same record. The Community Health Index (CHI) number is the unique patient identifier in all NHS Scotland systems, which will unite patients' records irrespective of where they have been created. Whilst departments currently have a plethora of different hospital numbers which are used to identify manual patient records, the relevance of these will diminish to that of a case record filing number as CHI becomes established throughout all healthcare settings. Work is ongoing across NHS Scotland via the CHI Programme to ensure that the CHI number is ubiquitously used across all sectors of NHS Scotland for patient identification and all clinical communication.

Patient Management System (PMS)

Currently across NHS Scotland there are multiple Patient Administration Systems (PAS) employed operationally in secondary and community care. PAS systems are used to administer patient record systems and are pivotal to effective records management in secondary and community hospital environments. All but one existing commercial PAS contract is due to expire between 2008 and 2010. NHS Scotland eHealth Strategy Board has agreed that a national approach should be taken to re-procurement of secondary and community care PAS. An outline business case has been prepared and circulated to Boards for consideration.

Features of the solution will include provision of 24/7 core PAS business functionality:

- patient identification;
- electronic referrals workflow management;
- scheduling;
- bed management;
- case record tracking;
- clinic attendances and in-patient management;
- document production;
- clinical coding;
- management reporting tools.

In addition the required solution is expected to include:

- integration with order communication and results reporting;
- integration with HEPMA electronic drugs prescribing, medicines administration and pharmacy modules;
- integrate with or interface to a number of other clinical modules;
- provision of facilities to users of locally and nationally managed accredited business systems;
- conformance to interoperability and data standards;
- future interface with IPACC (e.g. primary health care record, scheduling, mental health).

Clearly the move to a single patient management system across Scotland will provide the foundation for the creation of a national electronic patient record through the authentication of patient demographic data and records linkage.

6. Review

This strategy will be reviewed every two years (or sooner if new legislation, codes of practice or national standards are to be introduced).

The Scottish Health Records Forum acknowledges the effort of the sub-group in drafting this strategy for use across NHS Scotland. It is hoped the document will provide a framework which can be customised for use at individual NHS Board level.

Mr Robert H Bryden, NHS Ayrshire & Arran (Chair)
Miss May McConnell, NHS Ayrshire & Arran
Mrs Marilyn Horne, NHS Glasgow & Clyde
Ms Dorothy Ireland, NHS Forth Valley
Ms Elizabeth Lothian, NHS Forth Valley

ISBN 978 0 7559 1750 1 (web only publication)