Department of Health

Records Management:

NHS Code of Practice

Part 1

DH INFORMATION READER BOX

Policy HR/Workforce Management Planning Clinical	Estates Performance IM & T Finance Partnership Working
Document Purpose	Best Practice Guidance
ROCR Ref:	**Gateway Ref:** 6295
Title	Records Management: NHS Code of Practice
Author	DH/Digital Information Policy
Publication Date	30 March 2006
Target Audience	NHS Records Managers
Circulation List	PCT CEs, NHS Trust CEs, SHA CEs, Care Trust CEs, Foundation Trust CEs, Medical Directors, PCT PEC Chairs, NHS Trust Board Chairs, Special HA CEs, Directors of HR, Directors of Finance, Allied Health Professionals, GPs, Royal Colleges, BMA, GMC, Healthcare Commission
Description	The Code of Practice is a guide to the standards of practice required in the management of NHS records, based on current legal requirements and professional best practice. The guidance applies to all NHS records and contains details of the recommended minimum retention period for each record type
Cross Ref	HSC 1999/053 – For The Record HSC 1998/217 – Preservation, Retention and Destruction of GP General Medical Services Records Relating to Patients HSC 1998/153 – Using Electronic Patient Records in Hospitals: Legal Requirements and Good Practice
Superseded Docs	HSC 1999/053 – For The Record HSC 1998/217 – Preservation, Retention and Destruction of GP General Medical Services Records Relating to Patients HSC 1998/153 – Using Electronic Patient Records in Hospitals: Legal Requirements and Good Practice
Action Required	N/A
Timing	N/A
Contact Details	Liz Waddington Digital Information Policy NHS Connecting for Health liz.waddington@dh.gsi.gov.uk 0113 280 6748 recordsmanagement@dh.gsi.gov.uk
For Recipient's Use	

Records Management: NHS Code of Practice

Part 1

Contents

Section 1 – Foreword

1. The *Records Management: NHS Code of Practice* has been published by the Department of Health 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 England. It is based on current legal requirements and professional best practice.

2. The guidance was drafted by a working group made up of representatives from the Department of Health, NHS Connecting for Health, the Health Archives Group and in collaboration with a range of NHS organisations, including representatives from Acute Trusts, Primary Care Trusts, Strategic Health Authorities, GP practices and professional bodies.

3. The Code provides a key component of information governance arrangements for the NHS. 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.

Types of Record Covered by the Code of Practice

4. The guidelines contained in 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 healthcare sector) regardless of the media on which they are held. These may consist of:

   - patient health records (electronic or paper based, including those concerning all specialties, and GP medical records);
   - records of private patients seen on NHS premises;[1]
   - Accident & Emergency, birth, and all other registers;
   - theatre registers and minor operations (and other related) registers;
   - administrative records (including, for example, personnel, estates, financial and accounting records; notes associated with complaint-handling);

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

- X-ray and imaging reports, output and images;
- photographs, slides, and other images;
- microform (ie microfiche/microfilm);
- audio and video tapes, cassettes, CD-ROM etc;
- e-mails;
- computerised records;
- scanned records;
- text messages (both outgoing from the NHS and incoming responses from the patient).

Section 2 – Introduction

5. This Code of Practice replaces previous guidance as listed below:
   - HSC 1999/053 – *For the Record*.
   - HSC 1998/217 – *Preservation, Retention and Destruction of GP General Medical Services Records Relating to Patients* (Replacement for FHSL (94)(30)).
   - HSC 1998/153 – *Using Electronic Patient Records in Hospitals: Legal Requirements and Good Practice*.

6. The guidelines contained in this Code of Practice draw on advice and published guidance available from the Department for Constitutional Affairs (formerly the Lord Chancellor's Office) and The National Archives, and also from best practices followed by a wide range of organisations in both the public and private sectors. The guidelines provide a framework for consistent and effective records management that is standards based and fully integrated with other key information governance work areas.

7. NHS managers need to be able to demonstrate positive 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 facilitate and drive forward the necessary changes. Those responsible for monitoring NHS performance, for example Strategic Health Authorities (SHAs) and the Healthcare Commission, play a key role in ensuring that effective systems are in place.

8. The NHS is provided with support to deliver change. This includes:
   - *Setting and Achieving the NHS Standard for Records Management: A Roadmap*
     – this can be accessed directly at:

       http://www.dh.gov.uk/PolicyAndGuidance/OrganisationPolicy/RecordsManagement/fs/en
       or through the Information Governance Toolkit.

     The Roadmap is an integral part of this Code of Practice.

- Information Governance Toolkit
  - this has been updated to reflect the principles of this Code of Practice (from version 4 onwards).
- Information Governance policy and implementation teams within NHS Connecting for Health.

The Roadmap and Information Governance Toolkit are described in more detail at Annex A.

General Context

9. All NHS records are public records under the terms of the Public Records Act 1958 sections 3 (1)–(2). The Secretary of State for Health and all NHS organisations have a duty under the Public Records Act 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 Public Records, who is answerable to Parliament.

10. The National Archives is the body that is responsible for advising on the management of all types of public records, including NHS records. The National Archives has general oversight of the arrangements for the permanent preservation of records in local records offices, which have been formally approved by them as Places of Deposit (see Annex E).

11. The Introduction to The National Archives' *Records Management: Standards and Guidance* document states:

> "A systematic and planned approach to the management of records within an organisation, from the moment the need for a record to be created is identified, through its creation and maintenance to its ultimate disposal ensures that the organisation has ready access to reliable information. An organisation needs to maintain that information in a manner that effectively serves its own business needs, those of Government and of the citizen, and to dispose of the information efficiently when it is no longer required."

http://www.nationalarchives.gov.uk/recordsmanagement/advice/standards.htm

12. 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.

13. In addition, NHS organisations need robust records management procedures to meet the requirements set out under the Data Protection Act 1998 and the Freedom of Information Act 2000.

14. Records are a valuable resource because of the information they contain. High-quality information underpins the delivery of high-quality evidence-based healthcare, 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 that information, and in whatever media it is required. Information may be needed:

    - to support patient care and continuity of care;
    - to support day-to-day business which underpins the delivery of care;
    - to support evidence-based clinical practice;
    - to support sound administrative and managerial decision making, as part of the knowledge base for NHS services;
    - to meet legal requirements, including requests from patients under subject access provisions of the Data Protection Act or the Freedom of Information Act;
    - to assist clinical and other types of audits;
    - to support improvements in clinical effectiveness through research and also to support archival functions by taking account of the historical importance of material and the needs of future research; or
    - to support patient choice and control over treatment and services designed around patients.

15. This Code of Practice, together with the supporting annexes and in conjunction with the Roadmap, identifies the specific actions, managerial responsibilities, and minimum retention periods for the effective management of all types of NHS records (ie both corporate and health records) from creation, as well as day-to-day use of records, and storage, maintenance and ultimate disposal procedures.

Monitoring Records Management Performance

16. A number of bodies monitor NHS performance in respect of records management. The Healthcare Commission monitors a core governance standard relating to broad records management as part of its annual assessment of performance. The Audit Commission regularly conducts studies into records management and related information quality issues. The Department of Health collects performance details as part of the annual information governance assessment and these will inform the work of both the Healthcare Commission and the Audit Commission. The NHS Litigation Authority also undertakes a risk assessment survey as an integral part of the Clinical Negligence Scheme for Trusts (CNST).

17. Other bodies likely to comment on records management performance include the Health Service Ombudsman when investigating a complaint, and the Information Commissioner when investigating alleged breaches of Data Protection or Freedom of Information legislation or in promoting the Lord Chancellor's Code of Practice on Records Management under section 46 of the Freedom of Information Act.

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 a public record.

19. The 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 both 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.

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 an individual's name, address, age, race, religion, gender and physical, mental or sexual health.

21. Processing includes everything done with that information, ie holding, obtaining, recording, using, disclosing and sharing it. Using includes disposal, ie closure of the record, 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 professional regulatory bodies.

NHS Connecting for Health (NHS CFH)

23. The impact of the Government's health reform agenda will fundamentally affect the way the NHS approaches the management of all electronic records. The NHS Care Records Service (NHS CRS) and the establishment of Care Trusts are central to these reforms and will transform the way both health and social care information is managed.

24. NHS CFH is working to ensure that all NHS patient records will be kept in electronic format in the future. The NHS number has been adopted as the unique identifier for all patient records. Use of the NHS number will allow linkage of patient records across systems and organisations. It is envisaged that record linkage will improve effectiveness and efficiency of clinical care to patients. Use of the NHS number also supports the concept of a lifelong record. The NHS CFH's work programme is outlined in Annex B.

25. In the mixed economy of paper and electronic records which will exist as the NHS CRS is developed it is essential that paper and electronic records are managed consistently to ensure that a complete health record is available at the point of need. This transitional period, during which the balance of paper and electronic records will change, will generate significant challenges – for example before patient data is migrated to the national data spine the data must be validated to ensure that duplicate registrations are eliminated and measures put in place in local systems to ensure that duplicate registrations are not created in the future.

Social Care Records

26. Social Care records management is outside the scope of this Code of Practice. The good practice outlined is, however, applicable to all organisations, and colleagues from social care organisations are encouraged to adopt similar standards of practice. Relevant information for Social Care practitioners can be found within the 'Custodian' database (the repository of standards and related learning for local government); see:

    http://localegov.eibs.co.uk/custodian/social-care-blueprint

Section 3 – NHS Records Management

27. The aims of this NHS Code of Practice are:

- to establish an information governance framework for NHS records management in relation to the creation, use, storage, management and disposal of all types of records;
- to clarify the legal obligations that apply to NHS records;
- to explain the actions required by Chief Executives and other managers to fulfil these obligations;
- to explain the requirement to select records for permanent preservation;
- to set out recommended minimum periods for retention of all types of NHS records, regardless of the media on which they are held; and
- to indicate where further information on records management may be found.

Management and Organisational Responsibility

28. 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 adequate resources to achieve them.

29. A designated member of staff of appropriate seniority (ie Board level or reporting directly to a Board member) should have lead responsibility for records management within the organisation. This lead role should be formally acknowledged and made widely known throughout the organisation.

30. It is essential that 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 work areas.

31. All staff, whether clinical or administrative, must be appropriately trained so that they are fully aware of their personal responsibilities in respect of record keeping and records 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 hospital patient case-notes and who manage the 'records library' and other storage areas where records are kept, must have an up-to-date knowledge of, or access to expert advice on, the laws and guidelines concerning confidentiality, data protection (including subject access requests), and freedom of information.

Individual Responsibility

32. Under the Public Records Act all NHS employees are responsible for any records that they create or use in the course of their duties. Thus any records created by an employee of the NHS are public records and may be subject to both legal and professional obligations. A description of these obligations can be found in Annex C.

Policy and Strategy

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

34. 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.

35. 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.

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

Record Creation

37. Each operational unit (for example finance, estates, IT, healthcare) of an NHS organisation should have in place a process for documenting its activities in respect of records management. This process should take into account the legislative and regulatory environment in which the unit operates.

38. 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 authentication of the records so that the evidence derived from them is shown to be credible and authoritative.

39. 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.

Information Quality Assurance

40. It is important that all NHS organisations train staff appropriately and provide regular update training. In the context of records management and information quality, organisations need to ensure that their staff are fully trained in record creation, use 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 – to ensure that 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;

- the use of information – so staff understand what the records are used for (and therefore why timeliness, accuracy and completeness of recording is so important); and
- how to update information and add in information from other sources.

Record Keeping

41. 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 format(s) they are made accessible, and their relationship to organisational functions (for example finance, estates, IT, healthcare). An information survey or record audit is essential to meeting this requirement. This survey will also help to enhance control over the records, and provide valuable data for developing records appraisal and disposal policies and procedures.

42. 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.

43. 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.

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.

45. Storage accommodation for current records should be clean and tidy, should prevent damage to the records and should 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 readable information.

47. Equipment used to store current records on all types of media should provide storage that is safe and secure from unauthorised access and which meets health and safety and fire regulations, but which also allow maximum accessibility of 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 archiving policies and procedures in place for 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. For reasons of business efficiency or in order to address problems with storage space, NHS organisations may consider the option of scanning into electronic format records which exist in paper format. Where this is proposed, the factors to be taken into account include:

    - the 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 the local Place of Deposit or The National Archives with regard to records which may have archival value, as the value may include the format 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).

51. In order to fully realise the benefits of reduced storage requirements and business efficiency, organisations should consider disposing of paper records that have been copied into electronic format and stored in accordance with appropriate standards.

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. There are also a range of guidance documents (for example the Information Commissioner's *Use and Disclosure of Health Information*) that interpret statutory requirements and there may be staff within organisations who have special expertise in, or can advise on, particular types of disclosure.

53. Caldicott Guardians or their support staff should be involved in any proposed disclosure of confidential patient information, informed by the Department of Health publication *Confidentiality: NHS Code of Practice*. In GP surgeries, the responsibility for making decisions about disclosure ultimately rests with the GP. Data Protection officers may be available to advise on subject access requests by members of the public, and guidance on dealing with such requests is available on the Department of Health website:

    http://www.dh.gov.uk/PublicationsAndStatistics/Publications/PublicationsPolicyAndGuidance/PublicationsPolicyAndGuidanceArticle/fs/en?CONTENT_ID=4006743&chk=hHzm2w

54. These guidance documents and additional materials on freedom of information and other legislation can be found within the Information Governance Toolkit. See:

    http://nww.nhsia.nhs.uk/infogov/igt/

    NB currently available to NHS organisations only. The toolkit will shortly be moving to an internet site. Details will be published on the NHS Connecting for Health website:

    www.connectingforhealth.nhs.uk

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. Guidance can also be found within the Information Governance Toolkit. For GP records see *Good Practice Guidelines for General Practice Electronic Patient Records* (version 3.1), for guidance on the transfer of electronic patient records from one GP practice to another.

    http://www.dh.gov.uk/PublicationsAndStatistics/Publications/PublicationsPolicyAndGuidance/PublicationsPolicyAndGuidanceArticle/fs/en?CONTENT_ID=4008657&chk=rr8fQT

Retention and Disposal Arrangements

56. Detailed guidance on retention periods for a full range of NHS personal health and different types of business and corporate records is provided in Annex D.

57. 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.

Appraisal of Records

58. Appraisal refers to the process of determining whether records are worthy of permanent archival preservation. This should be undertaken in consultation with the organisation's own archivist (where such a post exists), or The National Archives, or with an approved Place of Deposit where there is an existing relationship.

59. Procedures should be put in place in all NHS organisations to ensure that appropriately trained personnel appraise records at the appropriate time. The retention schedules in Annex D outline the recommended minimum retention periods for all types of NHS records. 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.

60. Where there are records which have been omitted from the retention schedules, or when new types of records emerge, the Department of Health and/or The National Archives should be consulted. The National Archives will provide advice about records requiring permanent preservation.

61. 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 senior manager with appropriate training and experience who has an understanding of the operational area to which the record relates.

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

Record Closure

63. Records should be closed (ie 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.

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

Record Disposal

65. Each organisation should have a retention/disposal policy that is based on the retention schedules contained in this Code of Practice. The policy should be supported by, or linked to, the retention schedules, which should cover all records held by the organisation, including electronic records. Schedules should be arranged based on series or collections of records and should indicate the appropriate disposal action for all records (for example consult with The National Archives after 'x' years; destroy after 'y' years).

66. Records selected for archival preservation and no longer in regular use by the organisation should be transferred as soon as possible to an archival institution (for example a Place of Deposit – see Annex E) that has adequate storage and public access facilities.

67. Non-active records should be transferred no later than 30 years from creation of the record, as required by the Public Records Act.

68. 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 to the level of confidentiality or protective markings they bear. This can be undertaken on site or via an approved contractor.

69. It is the responsibility of the NHS organisation to ensure that the methods used throughout the destruction process provide adequate safeguards against the accidental loss or disclosure of the contents of the records. Most NHS records are confidential records. Contractors, if used, should be required to sign confidentiality undertakings and to produce written certification as proof of destruction. A British Standard Code of Practice for the secure destruction of confidential material is expected to be published in the summer of 2006.

70. 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.

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

Glossary of Records Management Terms

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)

The process of distinguishing records of continuing value from those of no value so that the latter may be eliminated. (The National Archives, Definitions in the Context of the Seamless Flow Programme)[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. (The National Archives, Records Management Standard RMS 3.1)

It is a legal requirement for NHS records selected as archives to be held in a repository approved by The National Archives; see Place of Deposit below.

[1] **Seamless Flow Programme, The National Archives**
The Seamless Flow Programme involves the creation of a seamless flow of digital records from creation in government departments, to preservation in the archives, through to delivery on the web. The programme is about linking together existing components and automating manual processes. The process of developing the seamless flow approach will allow the review and streamlining of other aspects of its architecture – notably catalogues and web searching. The development of an internet-based delivery system for digital records is a key component of The National Archives' response to the Government's 2005 target.

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 record creators are authorised and identifiable and that records are protected against unauthorised addition, deletion, alteration, use and concealment. (BS ISO 15489-1:2001(E))

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

Records necessary for conducting the current and ongoing 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 which retains their integrity and authenticity while ensuring that they remain accessible. (The National Archives, Definitions in the Context of the Seamless Flow Programme)

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.

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

A single record with a unique identifier containing information relating to the physical or mental health of a given patient 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 patient. This may comprise text, sound, image and/or paper and must contain sufficient information to support the diagnosis, justify the treatment and facilitate the ongoing care of the patient to whom 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 COMMISSIONER

The Information Commissioner enforces and oversees the Data Protection Act 1998 and the Freedom of Information Act 2000.

INFORMATION SURVEY/RECORDS AUDIT

A comprehensive gathering of information about records created or processed by an organisation. (The National Archives, Records Management Standards and Guidance – Introduction Standards for the Management of Government Records)

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 to:

- identify where and when health and other records are generated and stored within the organisation and how they are ultimately archived and/or disposed of; and
- 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 make them. Any unauthorised annotation, addition or deletion to a record should be explicitly identifiable and traceable.

JOINTLY HELD RECORDS

A record held jointly by health and social care professionals, for example in a Mental Health and Social Care Trust. A jointly held record should be retained for the longest period for that type of record, ie 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. Defined in ISO 15489 as "data describing context, content and structure of records and their management through time", metadata is structured information that enables the description, location, control and management of other information.

Metadata should include (amongst other details) elements such as the title, subject and description of a record, the creator and any contributors, and the date and format. For further information, see:

http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/pdf/metadatafinal.pdf

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.

http://www.govtalk.gov.uk/schemasstandards/metadata.asp

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, ie the person or department who actually takes, writes and issues the minutes.

MINUTES (REFERENCE COPIES)

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

NHS CARE RECORDS SERVICE

The NHS Care Records Service (NHS CRS) will connect all GPs, acute, community and mental health NHS trusts in a single, secure national system that will enable individual electronic patient record details to be accessed by authorised personnel, at the appropriate level, anywhere in England, via use of a unique identifier. The unique identifier to be employed throughout the NHS and its associated systems is the NHS number.

NHS NUMBER

Introduced in 1996, the NHS number is a unique 10 character number assigned to every individual registered with the NHS in England (and Wales). The first nine characters are the identifier and the tenth is a check digit used to confirm the number's validity. Babies born in England and Wales are allocated an NHS number by Maternity Units, at the point of Statutory Birth Notification.

The NHS number is used as the common identifier for patients across different NHS organisations and is a key component in the implementation of the NHS CRS.

NHS RECORDS (Public Records Act)

All NHS records are public records under the terms of the Public Records Act 1958 sections 3(1)–(2). All records created and used by NHS employees are public records.

PAPER RECORDS

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

PERMANENT RETENTION

Records may not ordinarily be retained for more than 30 years. However, the Public Records Act provides for records which are still in current use to be legally retained. Additionally, under separate legislation, records may need to be retained for longer than 30 years, for example Occupational Health Records relating to the COSSH (Control of Substances Hazardous to Health) Regulations, or records required for variant CJD surveillance.

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.

PLACE OF DEPOSIT

A record office which has been approved for the deposit of public records in accordance with section 4(1) of the Public Records Act 1958. This is usually the record office of the relevant (ie county, borough, or unitary) local authority. A list of those repositories recognised by The National Archives for the deposit of NHS archives is in Annex E. Contact details for them are to be found in the ARCHON directory on its website:

http://www.archon.nationalarchives.gov.uk/archon/

An organisation wishing to have records preserved as archives should consult with The National Archives in the first instance, unless that organisation has an existing working relationship with an approved Place of Deposit.

Some individual hospitals have themselves been appointed as a Place of Deposit. In practice, these have tended to be those larger hospitals which can commit the resources necessary to provide appropriate conditions of storage and access and to place them under the care of a professionally qualified archivist. The National Archives can provide advice to any organisation wishing to apply for Place of Deposit status. Further information about the work of archivists in NHS Trusts is available from the Health Archives Group.

PRESENTATION

The transfer to a third party (for example a University) of public records which have been rejected by The National Archives 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 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 or will be available in. Schemes must be approved by the Information Commissioner and reviewed periodically to make sure they are accurate and up to date.

PUBLIC RECORDS

Records as defined in the Public Records Act 1958 or subsequently determined as public records by The National Archives.

Records of NHS organisations (and those of predecessor bodies to NHS organisations) are defined as public records under the terms of the Public Records Act 1958 sections 3(1)–(2). NHS records are not owned by the NHS organisation that created them and may not be retained for longer than 30 years without formal approval by The National Archives. (The National Archives)

Records of services supplied within NHS organisations but by outside contractors are not defined as public records, but are subject to the Freedom of Information Act.

PUBLIC RECORDS ACT 1958

For further information, including the text of the Act, see The National Archives' website:

http://www.nationalarchives.gov.uk/policy/act

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 media) 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

A series is the main grouping of records with a common function or subject – formerly known as 'class'. (The National Archives)

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, because they 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))

http://www.ica.org/biblio/cds/isad_g_2e.pdf

A series comprises the record of all the activities that are instances of a single process. A series may be large or small: it is distinguished not by its size, but by the fact that it provides evidence of a particular process. If an activity takes place that is unique, rather than an instance of a process, its records form a series in their own right. (Elizabeth Shepherd and Geoffrey Yeo, Managing Records: a handbook of principles and practice (Facet 2003))

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. 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, including 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 either the application of a Freedom of Information Act exemption or a decision by The National Archives to restrict access where sensitivity, copyright or data protection issues arise. (The National Archives, Definitions in the Context of the Seamless Flow Programme)

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 eventual 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, transferred to an archival establishment, or presented to a third party (for example a University).

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))

Records identified as more appropriately held as archives should be offered to The National Archives, which will make a decision regarding their long-term preservation.

WEEDING

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

Annex A: 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, clients and service users by promoting the effective and appropriate use of information.

The Information Governance Framework enables NHS organisations in England, and individuals working within them, to ensure that personal information is dealt with legally, securely, effectively and efficiently in order to deliver the best possible care to patients, clients and service users. The focus is on setting standards and giving NHS organisations the tools to help them to incrementally achieve the defined requirements, make appropriate improvements to their service and ensure that that improvement is maintained.

The Information Governance Framework addresses a number of different aspects of NHS information handling over a number of key work areas, i.e. the Caldicott recommendations on the use of patient identifiable information, the Confidentiality Code of Practice, the Data Protection Act 1998, the Freedom of Information Act 2000, Information Management and Technology Security (ISO 17799 Code of Practice for Information Security Management), Health Records Management, Corporate Records Management and Information Quality Assurance. It provides a vehicle to develop clear standards, and directly links the standards to support and guidance materials and exemplar documentation.

The Information Governance Framework also allows 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, clients and service users 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 organisations can assess their compliance with current legislation, Government policy and national guidance. It has been approved by health ministers and the Review of Central Requirements Committee (ROCR).

The Healthcare Commission also uses the Toolkit as part of the standard to audit NHS organisations against the new core standards – Healthcare Commission: Criteria for Assessing Core Standards.

The Information Governance Framework details the standards expected of all NHS staff with respect to protecting clinical records from damage, destruction and inappropriate disclosure.

Setting and Achieving the NHS Standard for Records Management – A Roadmap

The Roadmap 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 Records Management: NHS Code of Practice. These include:

- an outline corporate records management strategy and implementation plan;
- an outline archiving strategy and implementation plan, including links to the work required to support the NHS Connecting for Health agenda;
- an appraisal of archiving/storage options;
- implementing electronic document management, including practical guidance on scanning;
- improving NHS number uptake in readiness for migration to the national data spine; and
- an overview of the revised requirements that will be incorporated into subsequent versions of the Information Governance Toolkit.

The content of the Roadmap will be reviewed and updated at regular intervals. The Roadmap is available electronically via the following weblink:

http://www.dh.gov.uk/PolicyAndGuidance/OrganisationPolicy/RecordsManagement/fs/en

Other Reference Material

1. The Lord Chancellor's Code of Practice under Section 46 of the Freedom of Information Act 2000. See:

   http://www.dca.gov.uk/foi/codemanrec.pdf

   The Code of Practice provides guidance to all public authorities as to the practice which it would, in the opinion of the Lord Chancellor, be desirable for them to follow in connection with the discharge of their functions under the Freedom of Information Act 2000.

2. The National Archives: *Model Action Plan for Developing Records Management Compliant with the Lord Chancellor's Code of Practice under Section 46 of the Freedom of Information Act 2000*. See:

   http://www.nationalarchives.gov.uk/policy/foi/pdf/national_health.rtf

   A records management action plan (produced by the Public Record Office, now The National Archives), detailing the steps that health service organisations should take to reach the standards set out in the Lord Chancellor's Code of Practice.

3. The National Archives: *Complying with the Records Management Code: Evaluation Workbook and Methodology* (March 2005)

   www.nationalarchives.gov.uk/news/stories/62.htm

   An evaluation workbook intended to be used to assess compliance with Part 1 of the Lord Chancellor's Code of Practice, issued under section 46 of the Freedom of Information Act 2000. The workbook can be used to assess records management practices across any type of organisation.

4. The National Archives: *File Creation*

   http://www.nationalarchives.gov.uk/recordsmanagement/advice/

   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.

5. ISO 15489 – international record keeping standards.

6. 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 at:

   http://www.govtalk.gov.uk

7. University of Edinburgh Records Management Section

   http://www.recordsmanagement.ed.ac.uk/InfoStaff/RMstaff/records_management_for_staff.htm

8. University of Edinburgh file naming conventions:

   http://www.recordsmanagement.ed.ac.uk/InfoStaff/RMstaff/RMprojects/AAPS/FileNameRules/FileNameRules.htm

   This document has been prepared as part of the AAPS 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.

9. Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically (BIP 0008: 2004 – Copyright BSI).

10. *NHS Health Record and Communication Practice Standards for Team-Based Care*. Launched by the NHS Information Standards Board, this details best practice from the Nursing and Midwifery Council, the General Medical Council and the Health Professions Council, to help ensure the recording and communication of patient information in a consistent way. It can be found at:

    http://www.isb.nhs.uk/pages/news010605.asp

11. Royal College of Physicians Record Keeping Standards:

    http://hiu.rcplondon.ac.uk/clinicalstandards/recordsstandards/

12. *Good Practice Guidelines for General Practice Electronic Patient Records* (version 3.1) – prepared by the Joint Computing Group of the General Practitioners Committee and the Royal College of General Practitioners, sponsored by the Department of Health. It can be found at:

    http://www.dh.gov.uk/PublicationsAndStatistics/Publications/PublicationsPolicyAndGuidance/PublicationsPolicyAndGuidanceArticle/fs/en?CONTENT_ID=4008657&chk=rr8fQT

13. The Royal College of Pathologists: *The Retention and Storage of Pathological Records and Archives* (3rd edition, 2005). See:

    http://www.rcpath.org/resources/pdf/retention-SEPT05.pdf

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

14. Recommendations for the retention of pharmacy records:

    http://www.pjonline.com/pdf/hp/200305/hp_200305_pharmacyrecords.pdf

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

    http://www.medicalprotection.org/assets/pdf/booklets/records_consultants_complete.pdf

16. *The NHS Care Record Guarantee*:

    http://www.connectingforhealth.nhs.uk/all_images_and_docs/crbb/crs_guarantee_2.pdf

    A document outlining the NHS commitment to respect patient rights, to protect patient confidentiality and to use patient information only for the purpose for which it was provided.

17. *Confidentiality and Disclosure of Information: General Medical Services (GMS), Personal Medical Services (PMS), and Alternative Provider Medical Services (APMS) Code of Practice, 24 March 2005*. See:

    http://www.dh.gov.uk/assetRoot/04/10/73/04/04107304.pdf

The Code of Practice sets out guidance on the use and disclosure of personal information held by independent contractors. It details the key information governance principles that should be followed when handling patients' and employees' personal information. The Code also sets out the legal basis for the sharing of personal information for the administration of healthcare and the forms in which that information may be shared, for example identifiable, or anonymised.

18. Information Commissioner: *Use and Disclosure of Health Data*

    http://www.ico.gov.uk/cms/DocumentUploads/use%20and%20disclosure%20of%20health%20data.pdf

19. Information Commissioner: *CCTV Code of Practice*

    http://www.informationcommissioner.gov.uk/cms/DocumentUploads/cctvcop1.pdf

    Images from CCTV should not be retained for longer than necessary. This requires that organisations look at the purpose of recording the images. The Information Commissioner outlines several scenarios that may require different retention periods. The document also sets out standards for storage of CCTV images that need to be retained for evidential purposes and for the access and disclosure of images to third parties.

20. *Confidentiality: NHS Code of Practice* (page 17)
    This details an overview of record keeping best practice, in respect of confidentiality. It can be found at:

    http://www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf

21. The Patient Information Advisory Group (PIAG)

    http://www.advisorybodies.doh.gov.uk/piag/

    Informed consent is the fundamental principle governing the use of patient identifiable information by any part of the NHS or research community.

    Guidance from the General Medical Council, the Medical Research Council, the British Medical Association and draft guidance from the office of the Information Commissioner reflect the evolving legal position and reinforce the requirement for consent.

Section 60 of the Health and Social Care Act 2001 provides a legal power to ensure that patient identifiable information needed to support essential NHS activity can be used without the consent of patients. The power can only be used to support medical purposes that are in the interests of patients or the wider public, where consent is not a practicable alternative and where anonymised information will not suffice. It is intended largely as a transitional measure whilst consent or anonymisation procedures are developed, and this is reinforced by the need to review each use of the power annually.

The PIAG's key responsibilities are:

- to advise the Secretary of State on regulations which should be made under section 60 of the Health and Social Care Act 2001;
- to advise the Secretary of State as required on the use of patient information and other NHS information; and
- to scrutinise carefully applications to use patient identifiable information made under section 60 to ensure that the criteria are met.

22. GP Quality and Outcomes Framework.
GP organisational indicators on records and information about patients. See:

http://www.dh.gov.uk/assetRoot/04/08/86/93/04088693.pdf

23. Registration Authority governance arrangements. See:

http://www.connectingforhealth.nhs.uk/implementation/registrationauthorities/

24. The National Joint Registry (NJR) is designed to record details of hip and knee replacement operations in England and Wales. It includes the NHS and the independent healthcare sector. The NJR uses an electronic system for collection, transfer and storage of data. The data fields (the NJR Minimum Dataset) are entered at source by each orthopaedic unit/hospital. For a patient's personal details to be submitted to the NJR, their informed consent must be obtained. The NJR provides a form for this purpose:

http://www.njrcentre.org.uk/

Useful Contacts

The National Archives

The National Archives, as both a government department and an executive agency, plays a central role in the public records system, in particular, in the selection of records. Their review work is undertaken across government, in accordance with the Public Records Act 1958, and is carried out under the supervision, guidance and co-ordination of the Keeper of Public Records.

This role was assigned to the Keeper in the light of the recommendations of the Grigg Committee on departmental records, which reported in 1954. Approximately 1.5km of shelving at The National Archives is filled with records from government departments each year. These records represent no more than 5% of the records created by these departments. Due to their strong local or specialist nature, some of the remainder are permanently preserved as public records, in 240 approved archives across the country. The great majority of records not selected for permanent preservation are destroyed.

For further information, see:

http://www.nationalarchives.gov.uk/recordsmanagement/selection/acquisition.htm#5

The Health Archives Group (HAG)

HAG is a representative body for archivists and records managers working in the health sector, including but not limited to the NHS. It has been an affiliated group of the Society of Archivists' Specialist Repositories Group since 2001. HAG aims to raise the profile of health archives and to improve the level of awareness in the NHS and elsewhere about record-keeping issues.

Further information about HAG, including current contact details, can be found on the Specialist Repositories Group section of the Society of Archivists' website:

http://www.archives.org.uk/

Institute of Health Record and Information Management (IHRIM)

Established in 1948, IHRIM provides qualifications at all levels, as well as career and professional assistance for members working in the field of health records, information, clinical coding and related professions.

IHRIM is an international, as well as national, organisation with members in many different countries around the world. Many members choose to study for the Institute's professional qualifications. IHRIM is also a founder member of The International Federation of Health Records Organisations (IFHRO) and the UK IFHRO Director serves on the General Assembly of the Federation.

www.ihrim.co.uk

Records Management Society of Great Britain

The Records Management Society was launched in 1983, in recognition of the ever-increasing number of people working in the fields of records and information management. Anyone concerned with records and information, regardless of their professional or organisational status or qualifications, can join the society. Organisations wishing to develop records or information systems and those that provide services in these fields are also able to join.

www.rms-gb.org.uk

Annex B: NHS Connecting for Health

The National Programme for IT, which is being delivered by the Department of Health agency NHS Connecting for Health, is bringing modern computer systems into the NHS to improve patient care and services.

The new IT systems and services being delivered are:

NHS Care Records Service (NHS CRS)

The NHS CRS is central to NHS reform and will transform the way health and social care information is managed. The service will provide an individual electronic NHS Care Record for every patient in England, securely accessible by the patient and those caring for them. It will give authorised health and care professionals access to patient information where and when it is needed. It will give patients access to all their health information and will mean they can be more involved in making decisions about their own care and treatment.

The 'Spine' is the name given to the national database of key information about a patient's health and care and it forms the core of the NHS CRS. More detailed information about all of a patient's contacts with the NHS will be held at the local level, where most healthcare is administered. The key nationally available information, together with the more detailed local information, combine to produce the complete care record of a patient.

Information held on the Spine allows care providers and patients to benefit from medical care when and where it is needed. It will include the key data crucial for each patient's care to commence or continue, such as an individual's:

- NHS number;
- date of birth;
- name and address;
- allergies;
- adverse drug reactions; and
- major treatments.

The Secondary Uses Service (SUS) is an important public health service provided through the NHS CRS, that will protect the confidentiality of patients and will provide timely, pseudonymised patient-based data and information for purposes other than direct clinical care, including:

- planning and commissioning;
- public health and research;
- clinical audit and governance;
- benchmarking; and
- performance improvement.

Electronic Booking Service (Choose and Book)

Choose and Book allows GPs and other primary care staff to make initial hospital or clinic outpatient appointments at a convenient time, date and place for the patient.

This enables patients to 'book' an appointment on the spot and leave the surgery with their appointment time and date. If preferred, patients can make their appointment later – after consulting with family carers or colleagues – either online or through a telephone booking service.

Electronic Transmission of Prescriptions (ETP)

The ETP service will connect prescribers and dispensers in primary care in England so that, by 2007, every GP surgery (ie the GPs, nurses and other prescribers working from the surgery) and community pharmacy and other dispensers will have access to the service. In due course, prescribers working from other locations, such as walk-in centres or dental practices, will also be included. There are also plans to include hospitals, to enable hospital prescriptions issued for dispensing in the community to be included.

The service will enable electronic prescriptions to be generated, transmitted and received so that pharmacists and other dispensers can dispense against them. Over time, dispensers will also be able to submit these electronic prescriptions to a reimbursement authority in order to claim payment. In many, and eventually most cases, electronic prescriptions will replace paper ones.

N3 – The National Network

N3 is the name for the new National Network, which replaces the private NHS communications network NHSnet. N3 provides fast, broadband networking services to the NHS, offering reliability and value-for-money. The new, high speed network will make it possible to deliver the reforms and new services needed to improve patient care, such as Choose and Book, NHS CRS, ETP and Picture Archiving and Communications System (PACS).

N3 is vital to the delivery of the National Programme for IT, providing the essential technical infrastructure through which the benefits to patients, clinicians and the NHS can be realised.

Picture Archiving and Communications System

PACS enables images such as X-rays and scans to be stored electronically and viewed on video screens, so that doctors and other health professionals can access the information and compare it with previous images at the touch of a button. By delivering more efficient imaging processes, PACS will contribute to the delivery of a maximum 18-week patient journey by 2008.

PACS technology allows for a near filmless process, with all of the flexibility of digital systems. It takes away the need to distribute images manually; images can be sent and viewed at one, or across several, NHS locations, enabling clinicians and care teams working together to view common information and so speeding up diagnosis. PACS also removes all the costs associated with hard film and releases valuable space currently used for storage. Most importantly, however, PACS has the potential to transform patients' experience of the care they receive across the NHS.

Contact

Contact is a secure national e-mail and directory service. It is provided free of charge for NHS staff and developed specifically to meet British Medical Association requirements for clinical e-mail between NHS organisations. *Contact* has been developed by the NHS with Cable and Wireless.

Contact is a quality e-mail service, with high availability and performance. It also provides other features:

- a national directory of people in the NHS, containing the name, e-mail addresses, telephone numbers, name and address of their NHS organisation, and information about departments, job roles and specialities;
- accessibility from anywhere on NHSnet or the internet, particularly useful for staff who work from more than one location;
- an e-mail address that stays with staff as they move around the NHS;
- calendars and folders that can be shared with other users across the NHS; and
- automatic encryption during sending of e-mails.

Contact has high standards of security – and email can safely replace paper communications such as:

- patient referrals from GP to hospital;
- hospital to hospital – or internal hospital referrals;
- discharge letters;
- clinical enquiries;
- research links; and
- clinical team communications.

Local procedures need to be in place at the sending and receiving ends of communication. Clinical information should be clearly marked and properly addressed. The receiver should be ready to handle information correctly and it should be stored securely and added to patients' records when appropriate. Information can be sent to a single individual or to a controlled group. *Contact* tracks what is received, by whom, and when it is read.

The Quality Management and Analysis System (QMAS)

QMAS is a new single, national IT system, which gives GP practices and Primary Care Trusts objective evidence and feedback on the quality of care delivered to patients. The system shows how well each practice is doing, measured against national achievement targets detailed in the General Medical Services (GMS) contract, which sets out the way GPs work and the way they are financially rewarded.

As GP practices are rewarded financially according to the quality of care they provide, it is essential that the payment rules that underpin the GMS contract are implemented consistently across all systems and all practices in England. QMAS ensures that this is achieved. QMAS allows GP practices to analyse the data they collect about the number of services and the quality of care they deliver, such as maternity services or chronic disease management clinics. This provides a positive incentive for GPs to treat patients in the community rather than referring them to hospital for treatment such as diagnosis or minor operations.

GP2GP

The General Practice to General Practice (GP2GP) is a project to enable the electronic component of a general practice patient health record to be transferred to a new practice when a patient registers with a new practice for primary healthcare.

GP2GP will offer a safer and more efficient service for patients, clinicians and their administrative support team. The benefits of using GP2GP are as follows:

- The patient health record will be available to the new GP a lot sooner (for example within 24 hours).
- The new GP will have knowledge of the patient's:
  - current medication;
  - drug interactions;
  - current problems; and
  - key past medical history.
- The system will improve patient safety.
- The system will increase patient confidence that they will get good continuing care.
- The system will prevent patients being asked for information that they have previously provided.

For further information on all NHS Connecting for Health delivery areas see:

www.connectingforhealth.nhs.uk

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. The key legal and professional obligations covering personal and other information listed in this Annex are as follows:

Relevant Standards and Guidelines

Professional Codes of Conduct

The Abortion 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.

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.

The Access to Health Records Act 1990

(See: http://www.dh.gov.uk/assetRoot/04/03/51/94/04035194.pdf)

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 not 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.

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.

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.

Administrative Law

(See the Department for Constitutional Affairs' guidance:

http://www.dca.gov.uk/foi/sharing/toolkit/lawguide.htm)

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. If not, its action is 'ultra vires', ie beyond its lawful powers. 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.

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.

Blood Safety and Quality Legislation

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

http://www.opsi.gov.uk/si/si2005/20050050.htm

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.

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

http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32002L0098:EN:HTML

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.

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.

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 magistrates' court, up to six months' imprisonment and/or a fine; or
- in the Crown 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.

The Civil Evidence Act 1995

This Act provides the legal basis for the use of documents and records of any format to be admissible as evidence in civil proceedings. This includes electronic patient records.

Statements contained within documents may be admissible even where the original document has been lost and only a copy is available.

Documents that form part of a record are also admissible as long as the public authority supplies a signed certificate verifying the authenticity of the document.

Records management considerations

A public authority is making a legal statement by authenticating such documents and records, therefore the organisation must be sure of the quality and reliability of an electronic record. It will therefore be important to be able to verify that the computer was not misused and was operating properly at the time the record was produced.

The Common Law Duty of Confidentiality

(See *Confidentiality: NHS Code of Practice*:

http://www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf)

Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence, it is also referred to as 'judge-made' or case law. 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, whether a disclosure is in the public interest is not a decision to be taken 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.

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 can 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.

Confidentiality: NHS Code of Practice

The Confidentiality Code of Practice is a result of a major public consultation that included patients, carers and citizens, the NHS, other healthcare providers, professional bodies and regulators.

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 Department of Health website at:

http://www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf

Disclosure after a patient's death

There are no clear legal obligations of confidentiality that apply to the deceased. Nevertheless the Department of Health and the General Medical Council agree 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 coroner 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 public records under the Public Records Act and it has been argued that they should be accessible under the Freedom of Information Act 2000. This issue is currently under consideration by the Department of Constitutional Affairs in conjunction with the Department of Health. Until the guidance is available, organisations should not release the health records of deceased patients unless it is to comply with the Access to Health Records Act.

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.

The Congenital Disabilities (Civil Liability) Act 1976

Where a child is born disabled due to negligent treatment of the mother during pregnancy, the child can bring a civil action for damages. This is a separate right to that of the mother. In such a case the limitation period only begins once the child has reached the age of 18 years and has resulted in damage to the child. The period may be extended where material facts are not known.

Records management considerations

Organisations need to take the provisions of this Act into account and ensure that the health records of all children and, in particular, the records of children born with a disability are not prematurely destroyed.

The Consumer Protection Act (CPA) 1987

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.

The general limitation period in respect of personal injury actions under the Limitation Act 1980 is:

- three years from the date on which the cause of action accrued – so 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 – ie the date when they realised that someone was potentially liable for the death.

Section 11A(3) of the Limitation Act 1980 provides that actions in respect of damages for defective products shall not be brought after the expiration of 10 years from the date of supply/manufacture etc in accordance with terms of s.4 CPA 1987.

Section 11A(4) provides that an action for damages for personal injury caused by a defective product, or of loss of, or damage to any property, shall not be later than:

- three years from the date the cause of action accrued; or
- three years from the date of knowledge of the injured person, whichever is the later.

However, it needs to be noted that section 33 of the Limitation Act 1980 provides a discretion to allow an action for damages for personal injury or death to proceed (including damages in respect of personal injury/death caused by a defective product) if there would otherwise be prejudice to a party to legal proceedings. This discretion does not extend to a claim for loss or damage to **property** caused by defective products.

Records management considerations

A claimant generally has three years to begin legal action after the damage, however this period may be extended to ten years after the product was supplied. 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.

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

(See: http://www.hse.gov.uk/coshh/index.htm)

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 D1.

The Copyright, Designs and Patents Act 1990

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.

The Crime and Disorder Act 1998

The Act provides for anti-social behaviour orders to be applied for by a police authority or a local authority against an individual aged 10 years and over. The Anti-Social Behaviour Act (2003) amends the 1998 Act to include a Strategic Health Authority, an NHS Trust and a Primary Care Trust. These can be applied for where that individual has acted in a manner that caused or was likely to cause harassment, alarm or distress to one or more persons not of the same household as himself. The function of the order is the protection of persons in the local government area from further anti-social acts by the individual.

Section 115 of this Act permits the disclosure of personal information that may otherwise be prohibited. There is not a compulsion to disclose and the organisation must make its own decision; however, the requirements of the common law duty of confidence and the Data Protection Act 1998 must still be met. Therefore, information given in confidence must not be disclosed unless there is a clear overriding public interest in doing so.

If a disclosure is to be made, the information must only be disclosed to a relevant authority.

The disclosure must be necessary or appropriate to allow the Crime and Disorder Act to be applied.

What is necessary or proportionate depends on the individual circumstances of each case. The outcome to be achieved in disclosing information must be weighed against the public interest in provision of a confidential health service by the NHS.

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.

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.

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 Trust 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:

- by completing the online form at:

  http://www.ico.gov.uk/eventual.aspx?id=322

  then printing it and posting to the Information Commissioner;
- by requesting a notification form from: http://www.ico.gov.uk/eventual.aspx?id=324; or
- by phoning the notification help line (01625 545 740).

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, ie 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 at nww.nhsia.nhs.uk/infogov/IGT. 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 disposal arrangements for the destruction, archiving and closure of records, and 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.

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. 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 them.

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.

If no permanent record is requested, no fee for access may be made to records that are accessible and 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 (ie 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

http://www.opsi.gov.uk/legislation/about_legislation.htm

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.

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 healthcare organisation at which the trial was carried out must retain the health records of the patients involved for the maximum period possible, ie 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.

The Disclosure of Adoption Information (Post-Commencement Adoptions) Regulations 2005

The regulations require that adoption agencies keep records on the adopted children they have placed for at least 100 years and places limits on the information that can be disclosed.

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.

The Environmental Information Regulations 2004

(See: www.defra.gov.uk/corporate/opengov/eir/index.htm)

The Environmental Information Regulations 2004 came into force at the same time as the Freedom of Information Act 2000 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 Act exempts environmental information from being dealt with under freedom of information and provides for it to be dealt with under the Environment Information 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 Act 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.
- All exemptions for refusing an EIR request are subject to a public interest test.

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

Records management considerations

As with the Freedom of Information Act 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.

The Freedom of Information Act (FOIA) 2000

(See: www.foi.gov.uk and www.ico.gov.uk)

The FOIA lays down requirements for public bodies (including the NHS) to keep and make information available on request. The new rights of access in the FOIA 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; and
- a duty on every public authority to adopt and maintain a scheme, which relates to the publication of information by the authority and is approved by the Information Commissioner.

Section 46 of the Act places a duty on the Lord Chancellor to issue a Code of Practice on records management. The Code has been published and although compliance is not obligatory, it provides guidance to all public authorities as to the practice which it would, in the opinion of the Lord Chancellor, be desirable for them to follow in connection with the discharge of their functions under the FOIA. Additionally, the Code will 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 confers two rights on the general public:

- the right to be informed whether a public body holds certain information; and
- the right to obtain a copy of that information.

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;
- 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.

Organisations may charge a fee for reasonably incurred costs to:

- inform the applicant whether it holds the information; and
- communicate the information to the applicant.

However, they are not obliged to charge a fee, and the Department of Constitutional Affairs suggests that where the costs incurred are minimal the fee should be waived. If a fee is required, this should be notified to the applicant and paid within three months of receipt of the notice, otherwise the public authority need not comply with the request.

A fee may be charged to cover:

- the cost of putting the information into the applicant's requested format, for example CD, or audio tape;
- photocopying and printing costs (set at no more than 10 pence per page); and
- postage or other transmission costs.

In calculating the cost, organisations are not permitted to take account of employee time required to carry out the work. Additionally, organisations may not charge for putting the information into another format if they are already under a duty to make information accessible under other legislation, for example the Disability Discrimination Act 1995.

There may be a few cases where the costs of meeting a request would exceed the appropriate limit, set at £450 (for central government the limit is £600). If this is the case, organisations are allowed to refuse to answer the request.

The time for compliance by the public authority is the 20th working day following receipt of the request or further information and/or the appropriate fee. This period can be altered by the Secretary of State (up to the 60th working day).

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

Publication scheme

A publication scheme should be a complete guide to the information routinely published by an organisation. It is a description of the information about the organisation which is made publicly available and which should act as a route map so that the public can easily find information about the organisation.

The publication scheme 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 FOIA 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.

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.

Further information is available from the Department of Constitutional Affairs at:

http://www.dca.gov.uk/constitution/transsex/index.htm

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) (England, Wales and Northern Ireland) (No. 2) 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 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.

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

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 from:

http://www.hsebooks.com/Books

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.

The Health and Social Care Act 2001

Section 60 of this Act enables the Secretary of State for Health to make regulations that require or allow patient information to be shared:

- for medical purposes; or
- to improve patient care and for public interest purposes.

Regulations under the Act may therefore be made to permit patient information to be processed in circumstances where consent cannot be obtained. The processing permitted is still subject to the Data Protection Act 1998; however, it does mean that the common law duty to obtain consent has been set aside.

Section 61 provides for the establishment of a statutory committee – the Patient Information Advisory Committee (PIAG). The Secretary of State is required to consult with PIAG before making any regulations under section 60.

Interested persons, for example researchers or database holders, are required to seek permission from PIAG to enable the lawful processing of patient information where it is impossible to obtain consent. Permission is not automatically granted. The applicant must show that their application will improve patient care or is in the public interest and detail why they are unable to either gain consent or use anonymised information.

Records management considerations

Procedures should be put in place to provide information under section 60 regulations and to inform anyone requesting patient identifiable information of the need to request permission from PIAG for purposes other than direct healthcare, unless they have explicit consent from the patient.

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).

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 their 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.

The Limitation Act 1980

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. This period runs from when it is first realised that a person has suffered a significant injury that may be attributable to the negligence of a third party or from 10 years after the application of a product that is found to be defective (see Consumer Protection Act).

The Congenital Disabilities (Civil Liability) Act 1976 (see above) clarifies the right of a child born disabled, as distinct from the right of his/her mother, to bring civil action for damages in respect of that disability. For a minor, the limitation period runs from the time he/she attains the age of 18 years and may be extended where material facts are not known.

A person of 'unsound mind', as long as he remains under the disability in question, can bring an action without limit of time through his 'next friend'. After the person's death, the period of limitation will run against his personal representative(s). Discharge from hospital does not imply that the person has fully recovered from the disability.

The limitation period of three years from the date of personal injury or death, or date of knowledge of a claim applies only to actions, that include a claim for damages in respect of personal injuries. In the case of other claims, for example a claim by a mentally disordered patient that he has been falsely imprisoned, the appropriate limitation period prescribed by section 2(1) of the Limitation Act 1980 is six years from the date when the patient ceases to be under a disability or dies.

For the purposes of the Limitation Act, a person of 'unsound mind' is a person who, because of mental disorder within the meaning of the Mental Health Act 1983, is incapable of managing and administering his property and affairs. This definition is consistent with the definition of 'disability' in the Supreme Court rules that prescribe how people under a disability may bring an action.

Records management considerations

A claimant generally has three years to begin legal action after the injury; however, the lapse between the 'injury' and 'knowledge' of it is without limit of time. Therefore, 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 The National Archives' guidance.

The NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000

Section 2 of these Directions repealed Regulation 2 of the National Health Service (Venereal Diseases) Directions 1991 and Annex B part 1 of the National Health Service Trusts (Venereal Diseases) Directions 1991.

The National Health Service (Venereal Diseases) Regulations 1974 (SI 1974/29) imposed on health authorities an obligation to ensure that information about sexually transmitted diseases obtained by their officers should be treated as confidential. In 1991, Directions were made imposing the same obligations on trustees and employees of an NHS Trust.

These new Directions, which apply only to England, impose the same obligations of confidentiality on the members and employees of both NHS Trusts and Primary Care Trusts.

Every NHS Trust and Primary Care Trust must take all necessary steps to ensure that any information capable of identifying an individual obtained by any of their members or employees with respect to persons examined or treated for any sexually transmitted disease shall not be disclosed except:

- for the purpose of communicating that information to a medical practitioner, or to a person employed under the direction of a medical practitioner in connection with the treatment of persons suffering from such disease or the prevention of the spread thereof; and
- for the purpose of such treatment or prevention.

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 might be included within past medical history (particularly hospital records).

The Police and Criminal Evidence (PACE) Act 1984

Under section 69 of this Act a statement in a document produced by a computer is not admissible as evidence in criminal legal proceedings unless it can be shown that:

- there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer; and
- at all times the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation did not affect the production of the document or the accuracy of its contents.

In other words, before a judge can decide whether computer printouts are admissible as evidence, it will be necessary to call appropriate authoritative evidence to describe the function and operation of the computer. This is normally a statement of evidence as to how the printout was obtained. A certificate signed by a person occupying a responsible position in relation to the operation of the computer will also be required; that person must state that the computer system was operating correctly at the time the evidence was obtained.

Records management considerations

Those responsible for managing any computer system from which information is requested which is to be used as evidence should be aware that they will need to provide a statement that the computer was operating properly at the time that the evidence was provided, or that any malfunction did not affect the production or accuracy of the document. They may also be requested to provide information on the function and operation of the system.

The Privacy and Electronic Communications (EC Directive) Regulations 2003

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 Information Commissioner.

Public Health (Control of Diseases) Act 1984 and Public Health (Infectious Diseases) Regulations 1988

Under this legislation, doctors in England and Wales have a statutory duty to notify a 'Proper Officer' of the local authority if they are aware that, or have cause to suspect that, a patient is suffering from one of the notifiable diseases. The doctor must complete a certificate stating:

- the name, age and sex of the patient and the address of the premises where the patient is;
- the notifiable condition from which the patient is, or is suspected to be, suffering;
- the date, or approximate date, of the onset of the condition; and
- if the premises are a hospital, the day on which the patient was admitted, the address of the premises from which he/she came there and whether or not, in the opinion of the person giving the certificate, the condition from which the patient is, or is suspected to be, suffering was contracted in hospital.

The list of notifiable diseases can be found on the Health Protection Agency's website at:

http://www.hpa.org.uk/infections/topics_az/noids/menu.htm

Records management considerations

Organisations should ensure that copies of the notification certificate or counterfoils from a notification book are held securely and retained for the recommended minimum period.

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.

The Public Records Act 1958

All NHS records, and those of NHS predecessor bodies, are public records under the terms of the Public Records Act 1958. The Act sets out broad responsibilities for everyone who works with such records, and provides for guidance and supervision by the Keeper of Public Records. It requires that those records that have been selected for archival preservation are transferred to The National Archives or a Place of Deposit appointed under the Act.

The maximum period for which records can be kept prior to transfer is usually 30 years (any NHS body that feels it needs to hold records for a longer period must consult with The National Archives). In practice, NHS records that have been selected for archival preservation are transferred to a Place of Deposit which is usually the record office of the relevant (ie county, borough or unitary) local authority. Some individual hospitals have themselves been appointed as a Place of Deposit, although these have tended to be those larger hospitals which can commit the resources necessary to provide appropriate conditions of storage and access and to place them under the care of a professionally qualified archivist.

Information about the most appropriate Place of Deposit for the records of particular NHS institutions can be obtained from:

Head of Archive Inspection
The National Archives, Kew, Richmond, Surrey TW9 4DU
Email: enquiry@nationalarchives.gov.uk
Tel: 020 8876 3444

Records management considerations

The Freedom of Information Act 2000 repealed s5 of this Act concerning access to public records. Further guidance is given in the introduction to the retention schedules in this Code of Practice (see Annex D).

The Radioactive Substances Act 1993

http://www.opsi.gov.uk/acts/acts1993/Ukpga_19930012_en_1.htm

The High-activity Sealed Radioactive Sources and Orphan Sources Regulations

http://www.opsi.gov.uk/si/si2005/20052686.htm

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.

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.

The Re-use of Public Sector Information Regulations 2005

The Regulations link with the Freedom of Information Act 2000, 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 the Freedom of Information Act 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.

Further information about the Regulations can be obtained from the Office of Public Sector Information at:

www.opsi.gov.uk

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 Act 2000); 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.

The Sexual Offences (Amendment) Act 1976 Subsection 4(1) as Amended by the Criminal Justice Act 1988

This prohibits the release of any information that would identify any rape victim for the lifetime of the victim.

Relevant Standards and Guidelines

BSI BIP 0008

The current British Standard document relating to 'Legal Admissibility and Evidential Weight of Information Stored Electronically'. It sets a benchmark for procedures that should be followed in order to achieve best practice.

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.

BS 4743

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.

BS 5454:2000

This makes recommendations for the storage of archival documents.

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.

ISO 15489

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

ISO 19005 – Document Management

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

The NHS Information Governance Toolkit

The Information Governance Toolkit return is required from all NHS organisations and provides guidance and best practice on all facets of information governance including:

- Data Protection Act 1998
- Freedom of Information Act 2000
- The NHS Confidentiality Code of Practice
- Records Management
- Information Quality Assurance
- Information Security
- Information Governance Management.

See: http://nww.nhsia.nhs.uk/infogov/igt/

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.

The General Medical Council

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

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.

See link: http://www.nmc-uk.org/(sknklt551haimf55pdsrmd25)/aFrameDisplay.aspx?DocumentID=475

The Chartered Society of Physiotherapy: Rules of Professional Conduct

http://www.csp.org.uk/director/effectivepractice/rulesofconduct/professionalconduct.cfm

General Social Care Council: Codes of Practice for Social Care Workers and Employers

http://www.gscc.org.uk/Good+practice+and+conduct/What+are+the+codes+of+practice/

Information on ethical practice

This can be obtained from the British Medical Association at:

http://www.bma.org.uk/ap.nsf/Content/Hubethics

Information on record keeping can also be obtained from the following:

Nursing and Midwifery Council (NMC) Guidance 01.05

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

http://www.nmc-uk.org/(k452wr55m2qj1p2ppgy3xf45)/aDisplayDocument.aspx?DocumentID=1120

Midwives' Rules and Standards – NMC Standards 05.04

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. See:

http://www.nmc-uk.org/(k452wr55m2qj1p2ppgy3xf45)/aDisplayDocument.aspx?DocumentID=169

270422/1 1p 5k Apr06 (CWP)
Produced by COI for the Department of Health

If you require further copies of this title quote
270422/1/*Records Management: NHS Code of Practice Part 1* and contact

DH Publications Orderline
PO Box 777 London SE1 6XH
Email: dh@prolog.uk.com

Tel: 08701 555 455
Fax: 01623 724 524
Textphone: 08700 102 870 (8am to 6pm Monday to Friday)

270422/1/*Records Management: NHS Code of Practice Part 1*
may also be made available on request in Braille,
on audio, on disk and in large print.

www.dh.gov.uk/publications