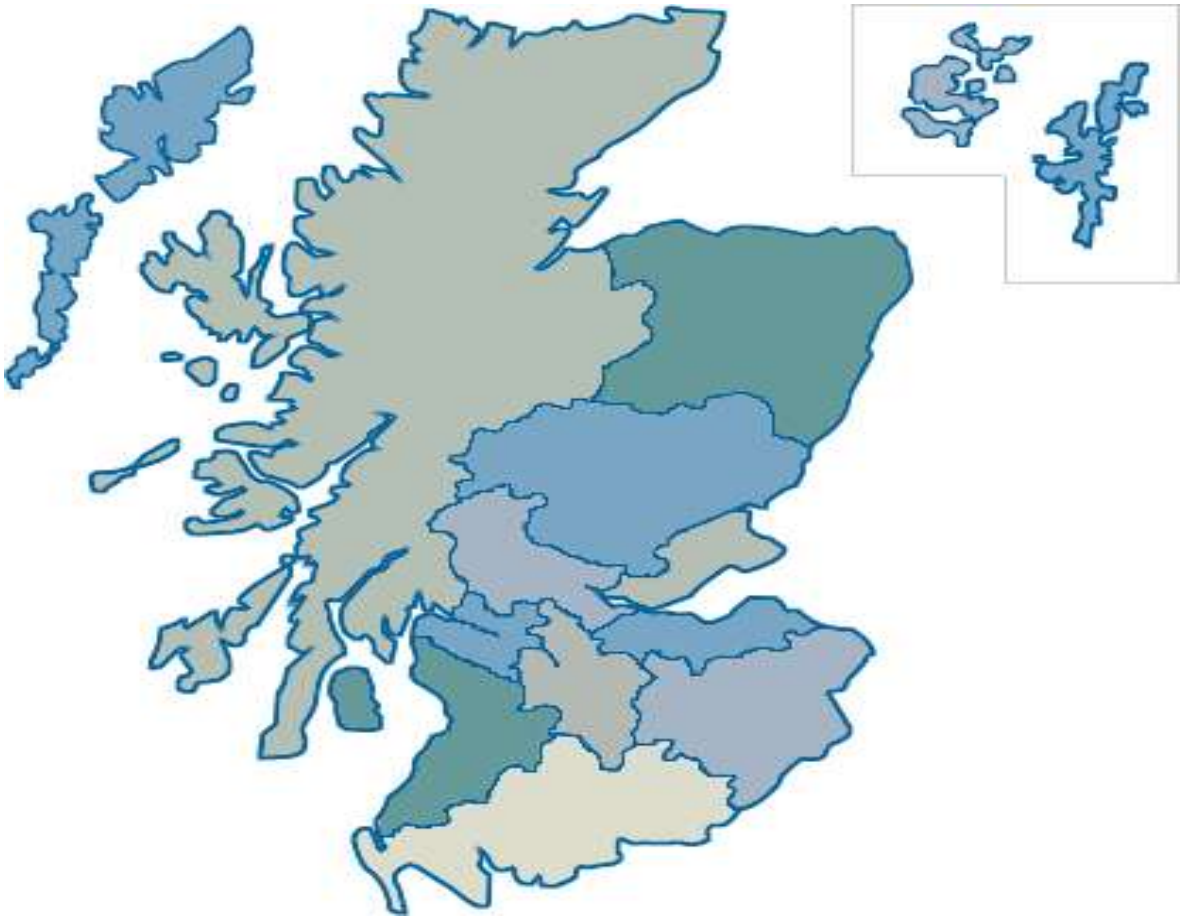
NHSScotland Caldicott Guardians: Principles into Practice



Foundation Manual for NHSScotland Caldicott Guardians
http://www.knowledge.scot.nhs.uk/caldicottguardians.aspx

FOREWORD

The delivery of "*world leading quality healthcare services*[1]" depends on sharing information among professionals and sometimes with external organisations. It is essential that the information that underpins the provision of healthcare is of a high quality and is shared to the benefit of the individual and wider society, making the role of the Caldicott Guardian increasingly important.

I am therefore delighted to have been asked to provide a foreword for the work which has been undertaken here in Scotland to build upon the caldicott principles; to reiterate them and to provide you, the Caldicott Guardian, with tools which I hope will be of real value to you; making it easier to fulfil your role locally.

This manual has been revised to meet the wider concerns identified by the Caldicott community regarding the confidentiality and security of patient information and appropriate, legal information sharing.

All of these areas fall within the duties of the Caldicott Guardian or those carrying out similar roles. This **Foundation Manual** tells you ***what you need to do*** and ***why you need to do it*** while the new Caldicott Guardian ***website*** shows you ***how to do it*** - providing advice, guidance, exemplar policies and other resources.

I am very appreciative of all the work that has produced the updated guidance and website and extend my thanks to everyone responsible.

Dr Harry Burns
Chief Medical Officer

[1] The Healthcare Quality Strategy for NHSScotland, The Scottish Government, May 2010

INDEX

This manual is supported by the NHSS Caldicott Guardian website " *Principles into Practice*" which is accessible at:
http://www.knowledge.scot.nhs.uk/caldicottguardians.aspx

1. Introduction

1.1. The 1997 Caldicott report made a number of recommendations for regulating the use and transfer of person identifiable information between NHS organisations and between NHS organisations and non-NHS bodies. The Caldicott Committee's remit included all patient-identifiable information passing between organisations for purposes other than direct care, medical research or where there was a statutory requirement for information. The aim was to ensure that patient-identifiable information was shared only for justified purposes and that only the minimum necessary information was shared in each case. The Committee also advised on where action to minimise risks of confidentiality would be desirable.

The recommendations of the Caldicott Committee influenced the confidentiality agenda for NHS organisations for a number of years. Central to the recommendations was the appointment in each NHS organisation of a "Guardian" to oversee the arrangements for the use and sharing of patient identifiable information. In Scotland these recommendations did not apply to Local Authorities. A key recommendation was that use of patient-identifiable information should be regularly justified and routinely tested against the following principles:

Principle 1 - Justify the purpose(s) for using confidential information
Principle 2 - Only use it when absolutely necessary
Principle 3 - Use the minimum that is required
Principle 4 - Access should be on a strict need-to-know basis
Principle 5 - Everyone must understand his or her responsibilities
Principle 6 - Understand and comply with the law

Since then developments in information management in NHSScotland (NHSS) have added to the Caldicott role including:

- Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information (Scotland) Act 2002
- NHSS Code of Practice on Protecting Patient Confidentiality.
- NHSS Information Governance standards 2005
- e-health developments (such as the ECS , SCI Store, SCI DC etc)

This manual takes account of these developments and, importantly, sets the role of the Caldicott Guardian within an organisational Caldicott/Confidentiality function which is itself a part of the broader Information Governance agenda.

This manual does not aim to reproduce or codify all the guidance available, but it updates existing materials where necessary and provides pointers to other current sources of guidance and standards which are available via the Caldicott Guardian website. The website is intended to be a 'one stop shop' for template policies and procedures, and links to legislation, Codes of Practice and Professional Standards.

The manual and website replaces the UK Caldicott Guardian manual. The new Caldicott Guardian manual and website will be subject to regular review and updated as necessary.

2. Who should be the Caldicott Guardian?

The Caldicott Guardian will be in priority order:

- an existing member of the management board of the organisation
- a senior health professional
- an individual with responsibility for promoting clinical governance within the organisation

Please see: **NHS Scotland Information Governance Standard 7.001**

2.1 It is particularly important that the Guardian has the seniority and authority to exercise the necessary influence on policy and strategic planning and carry the confidence of his or her colleagues.

All GP or Dental Practices, Opticians and Pharmacists must meet their information governance obligations. The Medical Director of the aforementioned may take up the role of Caldicott Guardian. All patients have a right to expect that information relating to them will be properly created and managed; that it will be handled in confidence and that patient-identifiable information will only be shared with those whose justification for receiving such information has been rigorously tested

2.2 Responsibility for ensuring that patient-identifiable information remains confidential is both an organisational and individual one. It is the responsibility of the Caldicott Guardian to facilitate understanding and awareness of that responsibility and to ensure that all such activities within an organisation are lawful.

Please see: NHS Scotland Information Governance Standards – 7.005

2.3 The specialist area of Information Governance is an integral part of activity within the NHS. It is here that most of the day-to-day actions governed by expectations of confidentiality and the protection of patient-identifiable information take place and here that responsibility usually lies for the appropriate polices and procedures which should operate throughout the NHS body. Each organisation must put in place an Information Governance Strategy and supporting policies which will enable the organisation to meet its legislative requirements and ensure operational and management information is timely, robust and reliable.

3. Role of the Caldicott Guardian?

3.1 The Caldicott Guardian plays a key operational role in ensuring that NHSS and partner organisations satisfy the highest practical standards for handling patient identifiable information.

Acting as the 'conscience' of an organisation, the Guardian should also actively support work to facilitate and enable information sharing, advising on options for lawful and ethical processing of information as required. Local issues will inevitably arise for Caldicott Guardians to resolve. Many of these will relate to the legal and ethical decisions required to ensure appropriate information sharing. It is essential in these circumstances for Guardians to know when and where to seek advice.

In all but the smallest organisations the Caldicott Guardian should work as part of a broader Information Governance function with support staff, Caldicott or Information Governance leads e.g. Data Protection Officers, Freedom of Information leads, Health Records Managers and IT Security staff contributing to the work as required.

3.2 Key Caldicott Responsibilities

The Caldicott Guardian also has a strategic role, however, that it is less appropriate to delegate.

Strategy & Governance: • Acts as an advisor and accountable for that advice • Sit on an organisation's Information Governance Board/Group or equivalent • Ensure that governance arrangements regarding Information Governance are in place and are effective in their organisation • Advise the Management team or the CEO of any issues relating to confidentialty assurance so they can be included in the Statement of Internal Controls. • Act as enabler for appropriate information sharing.
Confidentiality & Data Protection expertise: • Ensure that confidentiality issues are raised and minuted at Board / management team level, • Ensure that results/implications of internal and external audits relating to confidentialty and DP assurance and options for improvement where necessary are raised at Board • Develop a knowledge of confidentiality and data protection matters, drawing support from subject topic experts working within the organisation and external sources of advice and guidance where available.
Information Processing: • Oversees the confidentiality assurance requirements within IG Toolkit • Ensures that annual IG performance assessments are undertaken by staff involved in the Caldicott function • Ensure that confidentiality issues are appropriately reflected in organisational

strategies, policies and working procedures for staff.

Information Sharing:

- Provide advice on individual cases where there are any concerns about the potential for the disclosure of patient-identifiable information.
- Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within and outside the NHS e.g. disclosure to research interests and other agencies e.g. the police
- Oversee all arrangements to ensure that Information Governance is embedded in all clinical and research governance.

3.3 Please see: **Job profile of Caldicott Guardian** – The UK Council of Caldicott Guardians have endorsed a job description NHS Caldicott Guardians

3.4 The CHI Number

3.4.1 It is NHSS policy that a verified CHI Number is allocated to every patient at the beginning of their journey through the NHS, and that it is used in all records associated with every episode of healthcare. This is the only number which is to be used in clinical communications.

The Caldicott Guardian should ensure that the organisation develops procedures for the determination, recording and use of verified CHI numbers for all 'Active' patients, which should be used for both internal and external communications. All care records must include the CHI number as the patient identifier.

Since it is recognised that there are some patients for whom it is difficult to establish a verified CHI number, the Caldicott Guardian should ensure that this is part of the programme of work undertaken under the heading information management and that this area is the focus of constant attention and continuing effort.

All procedure documentation should be regularly reviewed and updated as appropriate.

Please see: NHS Scotland Information Governance Standards 5.007

The Caldicott Guardian should either be directly involved in or have given documented delegated authority to a colleague to validate and authorise the clinical information assurance required for the implementation of new systems and services.

Please see: NHS Scotland Information Governance Standards 6.003

3.4.2 The Caldicott Guardian should ensure that they are notified of all research and clinical education activities to verify the appropriate use of personal identifiable information for these purposes, in line with the Caldicott principles and data protection requirements.

3.4.3 Given the potential scope for the volume of research projects, it is appropriate for the Caldicott Guardian to give documented delegated authority for this to a suitable senior colleague. Or where the organisation has a defined post in the organisation for Research and Development management, the Caldicott Guardian should ensure they work closely with the post holder and act as final arbiter where a research project is in dispute, in terms of its appropriateness or clinical validity.

Please see: NHS Scotland Information Governance Standards 7.003

Local projects for clinical education should seek the opinion of the Caldicott Guardian on aspects of clinical governance. Such projects are usually authorised by the Lead of the clinical service, e.g. Director of Post-Graduate Medical and Dental Education, Director of Nursing.

4. Legislation, Codes of Practice and Protocols

4.1 Caldicott Guardians and those who work closely with them in this dynamic area were not established by a specific Act of Parliament and so have no directly related legal basis for their functions. They do however have a complex framework of legislation, non-statutory Codes of Practice and Protocols which are the supporting mechanisms for everything they do. In this section of the Manual we identify the most important of these and explain in broad terms the duties and obligations they place on individuals and organisations working in or in partnership with the NHS who may have access to the patient record. Where more detailed explanations are given later in this Manual and on the associated website, references have been summarised or have not been included here in their entirety to reduce repetition.

4.2 Many of the benchmarks we talk about in this Manual have a basis in Administrative Law which governs the actions of public authorities. From well-established precedents we know that a public authority cannot do what it intends to do (its public task) unless it has the power to do so. If it does not have the necessary power and acts without it, it is acting outside the law i.e. *ultra vires*. Even where the powers are thought to exist, a public authority must exercise those powers for the purpose for which they were created or for purposes which are 'reasonably incidental' to the defined purpose.

4.3 These powers do not usually specify the role of the public authority in relation to the disclosure of information. It has therefore become common practice to introduce statutory gateways which deal with this lack of function of which the Data Protection Act 1998 is a good example. In the context of healthcare there is a specific medical purposes condition under Schedule 3 of the Data Protection Act which means that in most cases, where the processing of health information relates to medical and care purposes, explicit patient consent does not have to be obtained.

Where disclosure of patient-identifiable information is not specifically allowed under primary or administrative law then the Common Law Duty of Confidentiality applies.

4.4 Common Law is the law of precedent. It is not written down and relies on the application of the findings in previous Court cases decided by sheriffs/judges.

The Common Law Duty of Confidentiality therefore means that it has been established that, when there is an expectation of confidentiality between two parties (in this case the Health Professional and the Patient), that confidence will not generally be broken without the explicit consent of the patient. In practice all patient information, whether held on paper, computer, video or audio tape, or even when it is simply held in the memory of a Health Professional, must not normally be disclosed to a third party without the consent of the patient.

This duty applies regardless of has age, mental health or capacity.

There are however four sets of circumstances in which the disclosure of confidential information to a third party is lawful:

- where the patient has given consent
- where disclosure is in the overriding public interest
- where there is a legal duty to disclose for example by court order
- where there is a statutory basis which permits disclosure

Confidentiality

Health Professionals are usually aware of their duty of confidentiality in relation to one-to-one consultations and in relation to written health records or consultations; curtains are not sound – proof and other patients or staff are likely to overhear.

The Caldicott Guardian must make sure that colleagues are aware of the need to comply with the common law duty of confidentiality at all times and not just in relation to formal records. On the other hand there will be circumstances where information relating to a patient or patients should and can be released without breaching these principles. It is perfectly acceptable to include patient data which has been anonymised or depersonalised to support research projects or to answer requests for information – the concept of confidentiality of patient identifiable information should not be confused with the use and application of patient data which is not individually identifiable.

4.5 Disclosure in the Public Interest

An American citizen was found to have contracted TB just prior to coming to Europe for his honeymoon. He was strongly advised not to travel but decided to do so, flying first to England and then onto Italy.

Public Health Authorities only discovered what had happened after he had left the United States. They alerted their colleagues in England and Italy and it was decided to publish details of the individual because of the very real danger to the health of a large number of people as this person travelled around, particularly since he was known to be using airlines.

* The circumstances in this case are exceptional but it is the exception which proves the rule. There will occasionally be times when the balance of the public interest demands a breach of confidentiality in the ‘interest of the greater good’.

Clearly there will be circumstances in which it will not be possible or appropriate to obtain or rely on the consent of the patient. Where this is not possible an organisation may be able to rely on disclosure being in the overriding public interest. Here a judgement needs to be made between the rights of the patient, in the interest of providing appropriate care, the public interest in maintaining trust in a confidential service, and any overriding pubic interest in disclosure.

The public interest in maintaining trust in a confidential service is a very important principle and should only be breached in exceptional circumstances. Applying the

public interest test is not about considering what the public are interested in but about 'the greater good' taking the course of action which is believed to be the least dangerous. Any decision to disclose information without consent must always be capable of a robust defence must be justified on a case-by-case basis and must be fully documented.

If there is any concern at all that such disclosure might be unjustified then disclosure should be refused and the applicant referred to legal remedies which will include application to a Court. Far better to take this course of action than to disclose and realise later that a mistake has been made – once information has been disclosed there is no opportunity to get it back again!

If a disclosure is made which is not permitted by Statute, Common Law or approved process, the patient can bring a legal action against both the organisation and the individual concerned.

Any legal proceedings notified to public authorities relating to a request for patient-identifiable information should be urgently referred to legal advisers so that the interests of the public authority and, separately if appropriate, the patient, may be represented in any proceedings.

4.6 Disclosure by Court Order

The case of R (TB) v Stafford Crown Court and others was about a patient's clinical records and whether a NHS hospital trust should disclose them for the purpose of criminal proceedings. The Court held that where a disclosure application is made, the patient should herself be invited to respond to it.

The patient, a 14 year old girl referred to as 'TB', was a witness at the trial of a man changed with various sexual offences. The man, W, wanted to see her medical records, in order to look for information that might undermine her credibility. He was allowed to do so following a hearing of which TB was unaware and at which she was not represented.

The Divisional Court said TB should have been notified of the original disclosure hearing so that she could object to disclosure of her records; the judge had failed to take into account TB's Article 8 EHRC right to confidentiality. It was unreasonable to leave it to the NHS trust to present her arguments to court.

4.7 Research and Audit

Wherever possible patient-identifiable information should not be used for such purposes and would not therefore normally involve the disclosure of patient-identifiable information. Research Ethics Committees now routinely require patient information to be anonymised or pseudonymised. However, particular care should be taken with 'small number data' when even with anonymisation or depersonalisation it may still be possible to identify the patient. Further guidance relating to 'small number

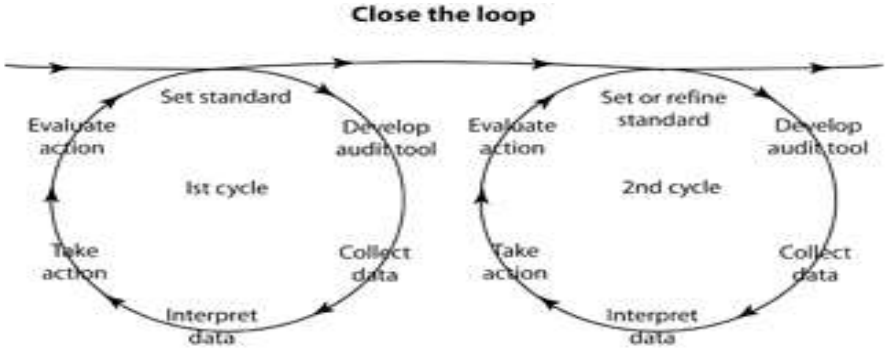
data' is available from the Office of National Statistics. The **ISD Statistical Disclosure Protocol** provides information regarding assessing and mitigation of the risk of identifying individuals in statistical publications.

Exceptionally it is necessary to use patient-identifiable or potentially identifiable information and responsibility for decisions regarding the appropriate use of such information lie with the data controller and their Caldicott Guardians. Scotland has no law defining acceptable purposes in these situations. The current approach is informed by '**Protecting Patient Confidentiality'**, the Report of the Confidentiality and Security Advisory Group 2002. In England acceptable purposes are defined in Section 251 of the NHS Act 2006 and advice on each case is provided to the relevant data controllers by the Ethics and Confidentiality Committee of the National Information Governance Board.

Currently there is no standard source of advice or procedure to assist data controllers in decisions regarding the use of information throughout Scotland. The **NSS Privacy Advisory Committee** advises NHS National Services Scotland regarding appropriate use of the national datasets. Researchers wishing to use these datasets apply to the Committee. Researchers who wish to use datasets controlled in other boards apply to each Caldicott Guardian individually where local procedures will apply.

Each NHS Board sets a programme of prioritised clinical audit for the year. The Clinical Governance Committee approves and monitors achievement of the clinical audit programme. Progress against the audit programme will also be used as an indicator of performance and as a basis for external monitoring/assessment.

Clinical audit is an ongoing cycle of continuous improvement. As a tool it suggests a number of questions about practice to help reflect, review and act to resolve problems and make changes to improve patient care. Clinical audit is often represented as an audit cycle or spiral.



Clinical audit is used to compare current practice with evidence of good practice. It can be used to make changes that improve the delivery of care. It can:

- Provide evidence of current practice against national SIGN guidelines or NHS Quality Improvement Scotland (NHS QIS) standards
- Provide information about the structures, the processes or outcomes of a healthcare service

- Assess how closely local practice resembles recommended practice
- Check "Are we actually doing what we think we are doing?"
- Provide evidence about the quality of care in a service to establish confidence amongst all of its stakeholders - staff, patients, carers, managers.

Clinical audit happens at different levels within an organisation. Audits can:

- Identify major risk, resource and service development implications in an NHS Board
- Reinforce implementation of evidence-based practice
- Influence improvements to individual patient care
- Provide assurance on the quality of care.

4.8. The NHS Code of Practice on Protecting Confidentiality: At a time when the emphasis is on sharing information, the Caldicott Guardian will need to ensure patients understand in what circumstances information is and where specific and informed consent will be sought.. This is of great importance and in Scotland guidance has been made available to all those dealing with confidentiality through the **NHS Code of Practice on Protecting Confidentiality**.

4.9. This Code of Practice recognises that while the provision and development of ever better healthcare is reliant on full, clear and accurate records, there will also be an ever-increasing requirement to share information. It reinforces the need for patients to be informed of the extent to which and with whom their information is being shared, their right to exercise choice over whether to give consent, and the importance of restricting such sharing of confidential information to those directly involved in their care.

This Code of Practice sets out four main requirements which must be met:

- Look after a patient's information
- Allow individuals to decide, where appropriate, whether their information can be disclosed or used in particular ways.
- Always look for better ways to protect inform and provide choice.
- Ensure that patients are aware of how their information will be used.

4.10. The Data Protection Act 1998

The Data Protection Act 1998 establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

4.10.1 What are personal data?

The Data Protection Act (DPA) 1998 relates to personal data, which is defined as data that relates to a living individual from which that individual could be identified either from that data alone or from that data in conjunction with other information in the possession of the Data Controller or information which would be reasonably accessible to anyone else.

Personal data includes such information as an individual's name, address, age, race, religion, gender and information relating to the individual's physical or mental health. The definition of personal data also includes expressions of opinions about individuals and indications of the intentions of persons in relation to individuals.

4.10.2 Overview

The Data Protection Act sets out a number of conditions which must be met before data can be processed. These are set out in Schedules 2 and 3 of the Act. To process any personal data a condition in Schedule 2 of the DPA needs to be met.
The Act goes further identifying certain kinds of data as Sensitive Personal Data which includes Health Records and introduces additional conditions for processing such data. These are set out in Schedule 3 of the DPA and the Data Protection (Processing of Sensitive Personal Data) Order 2000.

The Schedules and Order can be found under the Legislation section of the website processing of the data can take place.

4.10.3 The Data Controller

The Data Controller is the person who determines how and why personal information is processed. This is an organisational function but in practice the responsibility will lie with the Chief Executive or a GP or Dental Practice or an Opticians or Pharmacist, who acts on behalf of the organisation. For detail is available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf

It is an offence under the Data Protection Act to process personal data (including, patient-identifiable data) in any way until you have completed a Notification to the Information Commissioner. Notifications to the Information Commissioner form part of the Public Register of Data Controllers which is accessible via the Commissioner's website: **www.ico.gov.uk.**

4.10.4 Eight Principles underpin compliance with the Data Protection Act 1998

1. Personal data must be processed fairly and lawfully.

2. Personal data must be obtained for one or more specified and lawful purposes in any manner incompatible with that purpose.

3. Personal data must be adequate, relevant and not excessive.

4. Personal data must be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes must not be kept for longer than is necessary for that purpose and those purposes.

6. Personal data shall be processes 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 Community Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

These principles promote openness and fairness in the processing of personal information and they of course apply to patient-identifiable information.

4.10.5 Rights of the Data Subject

The Data Protection Act 1998 also grants rights to an individual in respect of information held about them by others. These are:

1 the rights of subject access – individuals can ask for information held about them and find out how information may be used and the likely recipients of such information

2 the right to prevent processing likely to cause unwarranted, substantial damage or distress

3 the right to prevent processing for the purposes of direct marketing

4 rights in relation to automated decision making

5 the right to take action to rectify, block, erase or destroy inaccurate personal information

6 the right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Data Protection Act 1998 has been contravened.

4.11 Health Rights Information Scotland - Public Information Leaflets

Health Rights Information Scotland (HRIS) is funded by the Scottish Government Health Directorates to produce information for patients in Scotland about their rights and responsibilities when using the NHS.

HRIS has produced a set of core NHSS leaflets on rights and responsibilities when using the NHS these include:

- The NHS and You
- Complaints,
- Confidentiality,
- Consent
- health records

There are separate versions of the leaflets for children and young people:

- Consent - your rights,
- Confidentiality - your rights
- Have your say - your right to be heard

Information is also available relating to the emergency care summary.
All of the information is produced by consulting with stakeholders including the public to make sure that it's as useful and useable as possible. The leaflets are also available in a variety of languages and formats and can be viewed at: http://www.hris.org.uk/

4.12 If such information is being processed, as in a health record, the individual has the right to:

- be given a description of the information being processed
- be told the purposes for which the information is being processed
- and be told those to whom such information has been or may be disclosed.

4.13 The individual also has the right to:

- have communicated to them the personal information held about them
- have communicated to them any information available to the Data Controller about the source of the information
- be informed by the Data Controller of the criteria built into any automated decision-making processes which use personal information.

4.14 Fees under the Data Protection Act

Under the Data Protection Act 1998 (Fees and Miscellaneous Provisions Regulations 2000), an individual can be charged to view their health records, or to be provided with a copy of them.

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

A statutory time limit is imposed by the Act, in most cases requests for access to health records must be completed within 40 calendar days.

It is essential that before personal information is disclosed in response to a subject access request all possible avenues are explored to ensure that no other prohibition applies. Among these might be orders under S30 of the Data Protection Act 1998 which limit subject access to information relating to some health, education and social work records which may be restricted or denied under Subject Access Modification Orders. There will also be circumstances where information has been provided with expectations of confidence by other third parties. In such circumstances and if appropriate the view of the third party involved should be sought and considered before any such information is disclosed. There is often confusion between patient-identifiable information relevant to the health record and other information which does not constitute personal data – whether of the applicant or a third party under the Data Protection Act 1998. – in such cases the information is not personal information and is not covered by a request.

Issues of Consent

The National Creutzfeldt – Jakob Disease (CJD) Surveillance Unit and London School of Hygiene and Tropical Medicine embarked on a study to determine the risk factors for CJD. Following research and Ethics Committee Approval (REC), GP's were asked to contact relatives of both CJD sufferers and healthy controls (of a similar age and sex to those with CJD) to ask for their consent to be contacted by the Surveillance Unit. Three quarters of the GPs asked declined to participate; however, only 16% of the controls contacted by their GP's agreed to be interviewed.

This low response may compromise the validity of this study using this control group. The researchers were unable to get REC approval to telephone non-responders as it was considered a breach of patient confidentiality.

See: **http://www.parliament.uk/documents/upload/POSTpn235.pdf**

4.15 Organisations cannot comply with the requirements of the Data Protection Act without having supporting policies and processes in place. These policies which should be part of the Information Management Strategy should:

- define all information covered by the DPA
- list all the DPA principles
- outline the organisational policy for holding, obtaining, sharing, recording, using and storing personal or sensitive data
- provide guidance on the acceptable use of such information
- describe corporate and personal responsibility.

4.16 Access to Health Records Act 1990 – deceased patients

Only a small part of this legislation now remains after the implementation of the Data Protection Act 1998. It governs access to the medical records of deceased persons.

The duty of confidentiality remains after a patient has died.

Under the Access to Health Records Act 1990, the personal representative of the deceased and people who may have a claim arising from the patient's death are permitted access to the records. This applies to information provided after November 1991 and disclosure should be limited to that which is relevant to the claim in question.

4.17 Even where these tests are met this legislation does not grant a general right of access and there are circumstances which could limit disclosure:

- if there is evidence that the deceased did not wish for any part of their information to be disclosed
- if the disclosure would cause serious harm to the physical or mental health of any person
- if disclosure would identify a third party.

Please see link for further guidance: **Access to Health Records 1990 – deceased patients**

4.18 The Freedom of Information (Scotland) Act 2002

The **Freedom of Information (Scotland) Act 2002**(FOISA) came into force on 1 Jan 2005. The main features of the Act are:

- gives anyone from anywhere in the world - a general right of access to recorded information of any age held by a wide range of bodies across the public sector in Scotland, subject to certain conditions and exemptions;
- in relation to most exempt information, the information should only be withheld if the public interest in withholding it is greater than the public interest in releasing it;
- the creation of the office of Scottish Information Commissioner (the Commissioner), with wide powers to promote good practice and to enforce the rights created in the Act;
- a duty on each Scottish public authority to adopt and maintain a publication scheme, approved by the Scottish Information Commissioner. Publication schemes must specify the classes and manner in which information is, or is intended to be, published, together with an indication of whether the information will be available free of charge or on payment of a fee;
- a duty on the Scottish Ministers to issue Codes of Practice containing guidance on specific issues e.g. general duties and records management (under section 60 and 61 of the Act).

All requests for information to public authorities are requests under the Freedom of Information (Scotland) Act 2002 if they are in writing, there is a name and a contact address (an email address is sufficient) for response and you can broadly speaking understand what information is being requested.

The FOISA also imposes a statutory time limit within which requests must be dealt within (20 working days) and an upper limit applies to disproportionate costs for retrieving and collating information.

There is a strong interface with the DPA and with all other legislation which prohibits or limits the disclosure of personal information in any way.

4.19 If a request is for the Health Record of the patient themselves, the FOISA takes us along a pathway to DPA, Subject Access Requests and the process for dealing with requests from individuals asking about themselves. However, the FOISA also tells us what to do about requests for personal identifiable information from third parties i.e. not from the subject themselves. We should still apply the principles of the DPA as the criteria on which decisions are made.

4.20 It is necessary for all organisations to have specific policies that ensure compliance with the Freedom of Information (Scotland) Act 2002. These should be statements of the organisation's principles and mechanisms which the organisation has adopted. Detailed guidance for staff should be posted on the organisation's intranet and leaflets made available for patients and staff.

4.21 Applicants for information under both the Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002 have the opportunity to complain if they feel that either Act has not been complied with by an NHS organisation. The Data Protection Act can be taken through the NHS complaints procedure. FOISA goes through a review process.

4.22 The Human Rights Act 1998

The rights of data subjects are often discussed in the context of the **Human Rights Act 1998 (HRA)**. Article 8 of the HRA establishes a right to 'private and family life'. This principle goes hand-in-hand with the Requests for third party information.

Common Law Duty of Confidentiality and the importance of protecting the privacy of individuals and the confidentiality of their health and social care records. However, it is not the case that the Human Rights Act confers unlimited privacy. It is recognised that there are specified grounds on which it may be legitimate for authorities to limit or supersede those rights. It is generally accepted that compliance with the Data Protection Act 1998 and the common law duty of confidentiality will satisfy the requirements of the Human Rights Act 1998.

4.23 An important principle associated with the interpretation of the HRA when considering disclosure of confidential information is that of proportionality. Any proposal to waive the obligations of confidentiality by the application of legislation must:

- pursue a legitimate aim
- be considered necessary in a democratic society
- be proportionate to a specified need.

Any activity which interferes with the right to respect for private and family life by, for example, disclosing confidential information, must also be justified as being necessary to support legitimate aims and be proportionate to need.

Any action against a public authority alleging a breach of the HRA will require the public authority to demonstrate that in making the decision it was aware of and gave due consideration to the rights granted by the Act and that the reasons for setting these aside were justified.

4.24 In order to demonstrate that to be the case, any decision to interfere with the provisions of the HRA must be subject to a specific Test of Proportionality which balances the right of the individual to respect for their privacy with other important considerations such as the prevention and detection of crime or protecting others from harm. In this the demands of the HRA are closely associated with the Principles of the Data Protection Act.

4.25 These are the most significant of the Acts and Codes directly involved in the protection of patient-identifiable information. There are others which only assume importance in particular circumstances in which the Caldicott Guardian may occasionally be called upon to offer advice.

4.26 The Human Fertilisation and Embryology Act 1990, as amended by the Human Fertilisation and Embryology (Disclosure of Information) Act 1992.

Further amendments to this legislation were introduced in 2008 following a review and consultation but these are unlikely to affect the disclosure of information. One of the most important tenets remaining is that this Act is retrospective and applies to information created both before and after the Act was passed.

The 2008 Act mainly amends the Human Fertilisation and Embryology Act 1990. Key provisions of the 2008 Act is to:

- ensure that all human embryos outside the body – whatever the process used in their creation - are subject to regulation.
- ensure regulation of “human-admixed” embryos created from a combination of human and animal genetic material for research.
- ban sex selection of offspring for non-medical reasons. This puts into statute a ban on non-medical sex selection currently in place as a matter of HFEA policy. Sex selection is allowed for medical reasons – for example to avoid a serious disease that affects only boys

- recognise same-sex couples as legal parents of children conceived through the use of donated sperm, eggs or embryos. These provisions enable, for example, the civil partner of a woman who carries a child via IVF to be recognised as the child's legal parent.
- retain a duty to take account of the welfare of the child in providing fertility treatment, but replace the reference to "the need for a father" with "the need for supportive parenting" – hence valuing the role of all parents
- alter the restrictions on the use of HFEA-collected data to help enable follow-up research of infertility treatment.

In general terms the Act prohibits disclosure of information by current and former members of the Authority and employees relating to entries in the Register of the Authority or any information obtained with an expectation of confidentiality. A further Regulation, **The Human Fertilisation and Embryology Authority (Disclosure of Donor Information) Regulations 2004 (SI 1511)** limits the information which will be provided by the Authority to persons who have attained the age of 18 and who may have been born in consequence of treatment services under the Act.

4.27 The Law and Information Sharing

We have thus far largely concentrated on legislation and Codes of Practice which prohibit or limit access to patient identifiable information. However there are also important legislative mechanisms which lay out conditions which state where information should be shared. More information about these and other mechanisms can be accessed via the **Caldicott website**. For reference purposes, we have included the most important here:

4.28 The Abortion Regulations 1991 provide a statutory gateway for disclosure of certificates of opinion to the Chief Medical Officer as required by the Abortion Act 1967.

4.29 Multi Agency Public Protection Arrangements (MAPPAs) The Management of Offenders (Scotland) Act 2005 required the police, local authorities and the Scottish Prison Services (known as the 'Responsible Authorities') to jointly establish arrangements for the assessment and management of risk posed by sex offenders and violent offenders. In practice this will be undertaken by the establishment across Scotland of 'Multi Agency Public Protection Arrangements' or MAPPAs. As well as having implications for the responsible authorities (which includes health boards in the case of mentally disordered offenders), the MAPPA's have an impact and requirement for agencies who have a 'Duty to Co-operate' under the 2005 Act.

4.30 The Public Health (Scotland) Act 2008 updates the law on public health, enabling Scottish Ministers, health boards and local authorities to better protect public health in Scotland. It will also assist Scottish Ministers to meet their obligations under the International Health Regulations. The Act also makes provision relating to the use, sale or hire of sunbeds, clarifies statutory responsibility for the provision of mortuaries and post mortem facilities and amends the law on statutory nuisances.

4.31. The Gender Recognition (Disclosure of Information) Scotland Order 2005 is gateway legislation which allows disclosure of information to a health professional which is otherwise prohibited by the Gender Recognition Act 2004.

4.32. The Road Traffic Acts (RTAs) also make provision for the disclosure of information by NHS bodies to enable the recovery of any costs of treatment. RTAs also require the NHS to provide any information which it is in their power to give and which may lead to the identification of a driver who has committed an offence under the Acts.

Only the most important legislation has been dealt with in detail here but links are available on the website to other legislation which has some interface with the protection or disclosure of patient-identifiable information.

4.33. Gun and Knife Wounds raise issues that warrant special consideration with regards to the sharing of information with the police. The General Medical Council (GMC) requires doctors to inform the police or social services whenever they treat a patient who is a victim of gun or knife crime, particularly those under 18. **Guidance is available from the GMC** and also the **BMA**.

5. Records Management

5.1 The Scottish Government Records Management NHS Code of Practice provides guidance on the required standards of practice in the management of records for those who work within or under contract to NHS organisations in Scotland. It is based on legal requirements and professional best practice. The Code of Practice can be found **here.**

5.2 NHS Records Management and Information Lifecycle

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

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

5.3 Roles and Responsibilities for Records Management and Organisational Responsibility

The records management function should be recognised as a specific corporate responsibility within every NHS organisation. It should provide a managerial focus for records of all types in all formats, including electronic records, throughout their life cycle, from planning and creation through to ultimate disposal. It should have clearly defined responsibilities and objectives, and necessary resources to achieve them. Great care must be taken when transferring clinical records between one site and another e.g. for disposal and only receptacles approved for the storage and transportations of health records should be used to prevent such records falling into the wrong hands.

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

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

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

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

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

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

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

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

All Staff:

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

5.4 Training

All staff, whether clinical or administrative, must be appropriately trained so that they are fully aware of their personal responsibilities as individuals with respect to record keeping and management, and that they are competent to carry out their designated duties. This should include training for staff in the use of electronic records systems.

It should be done through both generic and specific training programmes, complemented by organisational policies and procedures and guidance documentation. For example, Health Records Managers who have lead responsibility for personal health records and the operational processes associated with the provision of a comprehensive health record service should have up-to-date knowledge of, or access to expert advice on, the laws, guidelines, standards and best practice relating to records management and informatics.

5.5 Policy and Strategy

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

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.

The policy should also:

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

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

For further advice you should contact your Local Health Records or Corporate Records Manager.

Alternatively, if you seek policy advice, in relation to the NHSS Code of Practice on Records Management, you may wish to contact:
Records Management Lead
eHealth Strategy Division
eHealth Directorate **robert.bryden@scotland.gsi.gov.uk**

6. Information Management

6.1 Information Governance

Information Governance is a framework for handling all information in a confidential and secure manner to appropriate ethical and quality standards. NHS Information Governance is one element of the **NHS Quality Improvement Clinical Governance and Risk Management standards.** These standards will assist NHS Boards to develop and improve Information Governance at local level. Information Governance has six main components:

- Information Governance Management
- Confidentiality and Data Protection
- Freedom of Information
- Records management
- Information Security
- Information Quality Assurance

6.2 Staff, skills and resources assigned to each of these assurance areas can be thought of as organisational functions. Caldicott Guardians are central to the Confidentiality and Data Protection function, so much so that this is often referred to as the Caldicott function. Examples of how a range of organisations have supported their Caldicott function can be accessed through links found on the accompanying website.

6.3 In addition to the key area of confidentiality and Data Protection, the Caldicott Guardian needs to provide input into the other areas of Information Governance. The reverse is also likely to be the case, with staff working on other aspects of Information Governance being well placed to contribute to confidentiality and Data Protection work. It is important that organisations put in place effective governance arrangements to ensure that the organisation's approach to information governance is coordinated and inclusive.

6.4 The review of Information Governance in Scotland has led to the development of the Information Governance standards and self-assessment Toolkit for NHSScotland. NHS Health Boards should have Information Governance steering groups or boards as outlined in the Information Governance Toolkit, and it is recommended that the Caldicott Guardian attends these meetings.

6.5 The NHS Scotland Information Governance Electronic Toolkit is an online self-assessment tool that all NHS Scotland organisations are required to complete on a bi-annual basis. The Toolkit enables NHS Boards/Special Health Boards to record progress against National Information Governance Standards.

The Information Governance Standards cover the following key areas:

- Policy and Planning
- Confidentiality
- Freedom of Information
- Records management – for both Corporate and Health Records
- Data Protection

- Caldicott
- Information Management
- Information Security
- Data Quality

It should be noted that section 7 of the Information Governance Standards concerns Caldicott Guardians.

6.6 The Statement on Internal Control is part of the annual assurance process on governance within NHS organisations. As part of this process NHS Boards need to identify sources of assurance and evidence of compliance to enable them to produce a meaningful statement on the system of internal control within an organisation. This would include an assessment of the effectiveness of the internal control and risk management arrangements covering overall good governance and the four specific strands of governance:

- Clinical Governance
- Staff Governance
- Financial Governance
- Information Governance

7. Information Governance Structures and Networking Opportunities

7.1 Caldicott Guardian Forum:

The bi-annual forum enables Guardians to share best practice, obtain the advice of their peers on pressing problems and identify whether issues are likely to be of national significance.

Examples of existing networking structures which may prove useful include:

Local Data Sharing Partnerships
http://www.scotland.gov.uk/Resource/Doc/115502/0028631.pdf

7.2 NHSScotland National Information Governance Business Meetings

Quarterly meetings established to bring together all those who are responsible for the elements of IG at Board level to share good practice and learn about new developments. Contact the NHSS IG Team at: NSS.infogov@nhs.net.

7.3 NHS National Services Scotland Privacy Advisory Committee

The Privacy Advisory Committee (PAC) has been established to advise NHS National Services Scotland and the General Register Office for Scotland (GROS) on the processing of patient information. PAC has five members, of whom three are lay members and two are from NHS Scotland. The committee meets twice a year and carries on most of its work by mail and email. Applications for access to data held by ISD and other divisions of National Services Scotland are scrutinised by PAC before permissions are granted.
More information on the role remit and membership of PAC can be found at http://www.isdscotland.org/isd/3048.html

7.4 CHI Advisory Group (CHIAG)

CHIAG was set up in 2005 at the request of the Chief Medical Officer (CMO). Its role is to advise CMO and the Directors of Public Health in NHS Scotland on access to and use of the data held on the Community Health Index (CHI) for various purposes including operational management of the NHS, audit and research. The Committee meets quarterly, has a wide membership from across the NHS (including Caldicott Guardians) and includes a number of lay members. It is chaired by a Director of Public Health.
See: http://www.chiadvisorygroup.scot.nhs.uk/ for more information on CHIAG.

7.5 NHS Central Register Governance Board

The NHSCR Governance Board was set up in 2005 by the Registrar General to oversee the management of the National Health Services Central Register (NHSCR). NHSCR is managed by the Registrar General on behalf of the NHS in Scotland. It was created at the inception of the National Health Service in 1948 when its primary use was to manage the transfer of patients' medical records between General Practitioners. The NHSCR now has a number of additional uses including tracing patients, linking health records and it is also used, with appropriate permissions, for some research studies. Visit: http://www.gro-scotland.gov.uk/national-health-service-central-register/consultation-nhscr-governance-board/index.html for more information on the NHSCR.

7.6 The UK Council of Caldicott Guardians

The Council is an elected body made up of Caldicott Guardians from health and social care from across the UK, including three representatives from NHSScotland.

The aims and objectives for the Council are:

- To be the national body for Caldicott Guardians
- To promote the roles and activities of Caldicott Guardians within the United Kingdom
- To be a forum for the exchange of information, views and experience amongst all Caldicott Guardians
- To seek, consider and to represent the views of Caldicott Guardians on matters of policy relating to the organisation and delivery of Information Governance
- To be a channel of communication upon Caldicott matters with national organisations concerned with the NHS, the independent health sector, local government and health and social care professionals
- To act as a resource centre, provide support and arrange learning opportunities for Caldicott Guardians, both current and of the future.

The council meets quarterly, with more information available on the website: http://www.knowledge.scot.nhs.uk/caldicottguardians.aspx

8. Training and Awareness

Some training courses available to Caldicott Guardians are listed below. These are provided for information only and are not endorsed by SGHD.

- **Edinburgh University and Royal College of Surgeons of Edinburgh – Health Information Governance Postgraduate Programme**

The aim of the programme is to equip participants with the knowledge and practical skills essential for developing and implementing the Information Governance Agenda in the NHS in the UK and frameworks and systems in place in other countries. This encompasses:

- Interpretation and application of key information governance related legislation and improvement and implementation of information governance procedures and processes at a strategic and operational level in a healthcare setting
- Enhancing information management and knowledge management processes and practices at an organisational level.

See the University of Edinburgh site:
http://www.fhi.rcsed.ac.uk/site/2688/default.aspx

- **General Medical Council**

Good Medical Practice in Action is an interactive web section which brings the GMC's ethical guidance to life. More information is available at: http://www.gmc-uk.org/guidance/case_studies.asp

- **BMJ Learning**

Primary care and hospital practitioners and Practice Staffs learning needs. Choose from both clinical and non-clinical modules, covering access to health records, data protection and confidentiality. To log on please visit: http://www.bmjlearning.com/planrecord/index.jsp

- **ISEB- Data Protection**

Provides a recognised industry qualification at certificate level for those with data protection responsibilities, as well as providing an effective conversation route for those needing to update their knowledge of and practice under the 1998 Data Protection Act. More details are available at: http://www.bcs.org/server.php?show=nav.6925

- **Law and Medical Ethics Course - Edinburgh Law School**

A seven or ten-week course, or as individual modules delivered entirely by distance learning. The programme is aimed at medical practitioners and assumes no prior knowledge of law. Further details of the programme, including cost and start dates can be found at: http://www.law.ed.ac.uk/ahrc/teaching/cpd/lawandmedicalethics/

Data Protection Courses and Freedom of Information Courses
http://www.law.ed.ac.uk/ahrc/teaching/cpd/dataprotection/

- **University of Glasgow - Masters in Medical Law (Distance Learning)**

The Masters in Medical Law (MML) provides an opportunity to engage in topical and frequently controversial issues in medical law and ethics, within a flexible learning environment. The MML is a part-time degree, taught over two years by online, interactive modules, attendance at two residential weekends each year, and a dissertation under supervision.

Further information is available from:
Ms Sarah Elliston
Tel: +44 (0)141 330 2696
Email: S.Elliston@law.gla.ac.uk

9. Appendices – Supplementary Guidance and Advice

9.1 The Guardian as a Gatekeeper

Once a Caldicott Guardian has procedures and systems in place to control access to patient information, the Guardian should have responsibility for agreeing who should have access to what. Although it is necessary to be realistic about the pace at which existing systems and procedures can be changed if there are significant resource implications, the introduction of the new procedures can provide the opportunity to set high standards from the onset.

9.2 Access Control

9.2.1 Access control is essential for ensuring that only authorised persons have:

- Physical access to computer hardware and equipment;
- Access to computer system utilities capable of over-riding system and application controls;
- Access to manual files containing confidential information;
- Access to computer files and databases containing confidential information about individuals.

9.2.2 Whilst the introduction of appropriate procedures and systems is likely to fall to information security officers, facilities management and building security etc, it is important that Caldicott Guardian's are aware of current organisational capacity and intentions, through the management audit. Detailed guidance on access controls can be found on the Caldicott Guardian website and also in the NHSS Information Security Policy.

9.3 Physical Access Controls

Physical security protection should be based on defined physical parameters and achieved through a series of strategically located barriers throughout the organisation. Critical installations should be protected, at the minimum by lock and key with only authorised staff permitted access.

9.3.1 This is primarily a concern for the information security officer and is covered in detail in the NHS Information Security Policy (NHS HDL (2006) 41).

9.4 Access to Confidential Information about Individuals

9.4.1 Access to person identifiable information should be restricted to those staff who have a justifiable need to know in order to effectively carry out their jobs. The Caldicott Principles underpin the approach that NHS organisations should develop and introduce at a pace that is sustainable locally.

- **Principle 1** – Justify the purpose (s) for using confidential information

- **Principle 2** - Only use it when absolutely necessary
- **Principle 3** – Use the minimum that is required
- **Principle 4** – Access should be on a strict need to know basis
- **Principle 5** – Everyone must understand their responsibilities
- **Principle 6** – Understand and comply with the law

9.4.2 Registered access levels can be used to further limit the access of authorised persons to the minimum information that they need to carry out the task or function. This is particularly relevant to information that is held electronically, but the principles apply to all records, e.g. staff that need access to manual files for filing purposes should not need to access the information already contained within the files.

9.4.3 There are also legal restrictions on those who may see certain patient – identifiable information. Only staff whose responsibilities include treatment of individual patients with such diseases, or those who are involved more widely with the treatment or prevention of disease, such as those employed by public health departments, should be permitted access to such information. Organisations should therefore develop procedures for filtering out and/or anonymising relevant records. (See safe-havens below)

9.5 Information/Data "Ownership"

9.5.1 It is best practice for each physical set of information, e.g. manual files, or logically discrete set of electronically held information e.g. a database, to be assigned to an "owner". The information security officer should keep an up to date register of data "owners" and the Guardian should be provided with a copy. A number of responsibilities should be associated with ownership, including:

- Identifying all the information/data in the set
- Identifying and justifying to the satisfaction of the Guardian, how the information/data can be used
- Agreeing with the Guardian who can access the information/data and what type of access each user is permitted

9.5.2 Details of other responsibilities of "data owners" – e.g. information classification, security measures and compliance with Data Protection legislation can be found within the NHSS Information Security Policy.

9.6 Access Levels and Registration

There should be formal and documented user registration and de-registration procedures, for access to all person-identifiable information held in confidence, where multiple users need access. Again, although this is mainly applicable to electronically held information, the principles extend to manual files.

9.6.2 It is particularly important that it is clear, at any point in time, just **who** should have access to **what** information. It should be possible to immediately change or remove the access rights of individuals who have changed jobs or left the

organisation and a formal process to regularly review users' access rights should be established. For information held in electronic form, each user should have a unique identifier (user-ID) for their personal and sole use. A unique user-ID ensures that all activities on the system can be traced to the individual responsible and audits of activity undertaken. Each user should also have a password. As long as they are kept secret, passwords are an effective and easily introduced security measure. Detailed guidance on the use and management of passwords, aimed primarily at information security officers, is included within the **NHS Information Security Policy**.

9.6.3 Ideally, systems should permit users to be given different levels of access, and this requirement should be carefully born in mind when introducing new systems or upgrading old ones. The example given above of the access required by a filing clerk demonstrates that the principle can be applied to manual records as easily as to that held on a computer. Procedures for checking that the level of access granted to an individual is appropriate and justifiable, in the context of the business purpose, should be put in place and the Guardian's approval sought (see Information "Ownership" above).

9.7 Incidents and Security Breaches

Detailed guidance on the management of security incidents is included within the NHSScotland Information Security Policy - NHS HDL (2006) 41 and is largely the responsibility of the Information Security Officer. Guardians should ensure, however, that all security incidents involving the unauthorised disclosure of confidential personal information are reported both to themselves and to their Chief Executive. Where appropriate, advice on the handling of such breaches of confidence should be sought from the Scottish Government eHealth Directorate.

9.8 Safe-Havens

9.8.1 To support the introduction of access controls within an organisation and adherence to legal restrictions on the disclosure of certain information a useful model to adopt for routine flows of information is the use of designated safe-havens. This model requires confidential information to be disclosed or accepted through designated safe-haven contact points.

9.8.2. When information is received, access controls and registered access levels agreed by the Guardian, should then determine which staff within the organisation should have access to what information (see Controlling Access). When information is disclosed by a designated safe-haven point to an equivalent point in another organisation, staff can be confident that agreed protocols will govern the use of the information from that point on.

9.8.3 Where it is not practicable for patient information to be routed in this way, the staff involved must be made aware of any relevant protocols and take responsibility both for adhering to them and for drawing the attention of others to the standards that should apply. This is particularly relevant when information is shared to directly support patient/client care as a perception that another organisation does not adhere

to the same rules of confidentiality can put barriers in the way of information sharing and undermine the effective provision of seamless care.

9.8.4 Safe-haven arrangements originated to support contracting procedures, and detailed guidance was provided in MEL(92)42. The safe-haven model should, over time, be extended to cover all procedures for transferring confidential patient/client information between organisations when the purpose is not directly related to the provision of care. Guardians should work with the information security officer and staff familiar with safe-haven procedures to consider how the wider use of these procedures might be promoted across the organisation.

9.8.5 Retention and disposal of information should be in line with the Scottish Government Health Department guidance.

9.8.6 The key principles, updated to incorporate the Guardian role, are that:

- Each organisation should establish safe-haven administrative arrangements to safeguard confidential person-identifiable information. This includes having one designated contact point per physical site. Ideally, all information exchanged between NHS organisations should pass between safe-haven contact points.

- All members of staff (including, for example, switchboard operators and post room staff) should be made aware, at least in general terms, of the policies and procedures surrounding safe-haven access.

- Safe-haven procedures should be fully documented, approved by the Guardian and agreed by senior management.

- Safe-haven procedures should be comprehensive and cover:

    - Management arrangements
    - Staff roles and responsibilities
    - Physical location and security
    - Procedures for handling information
    - Controls on disclosure of information
    - Storage, archiving and disposal of information

9.9 Privacy Impact Assessment

Projects that involve personal information or intrusive technologies inevitably give rise to privacy concerns. The cumulative effect of many such initiatives during recent decades has resulted in harm to public trust and to the reputations of organisations
Where the success of a project depends on people accepting, adopting and using a new system, process or programme, privacy concerns can raise significant risks to organisations. In order to address these risks, it is advisable to use a risk management technique commonly referred to as a Privacy Impact Assessment (PIA).

Purpose of PIA: to identify at an early stage of project development potential privacy risks so that steps to mitigate these risks can be designed into the project.

When: A PIA should be conducted at an early stage of a project.
Compliance checks, on the other hand, are usually performed later after business processes and rules have been specified sufficiently so that they can be assessed for their compliance with the law.

How: Integrate the PIA within the project plan as a whole, or within broader risk assessment and risk management activities.

How much effort: The scale of effort that is appropriate to invest in a PIA depends on the circumstances. A project with large inherent risks warrants much more investment than one with a limited privacy impact. Other projects may merely need a check of their compliance with privacy laws, and in particular with the provisions of the Data Protection Act.

Who: The PIA is carried out by the Project or Programme Manager, taking advice from the Information Governance specialists within the organisation.

Role of Caldicott Guardian: Needs to be involved in any new projects relating to patient identifiable information:

- establish information flows
- ensure that data quality standards are being met and
- protocols relating to security and information sharing are in place .

Further Information: The ICO Privacy Impact Assessment (PIA) handbook is available at:
http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html