
Scottish Version

1.0
# Controls Template

## Document Information

<table>
<thead>
<tr>
<th><strong>Issue Date</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version/Issue Number</strong></td>
<td>Version 1.0</td>
</tr>
<tr>
<td><strong>Effective From Date</strong></td>
<td>July 2008</td>
</tr>
<tr>
<td><strong>Document Status (Draft or Final)</strong></td>
<td>Final 2008 update</td>
</tr>
<tr>
<td><strong>Circulation Level</strong></td>
<td>NHSScotland Caldicott Guardians</td>
</tr>
</tbody>
</table>
| **Consultation** | SGHD eHealth Directorate  
UK Council of Caldicott Guardians  
NHSScotland Caldicott Guardians  
NHSScotland Information Governance team |

### Scope of Document

This manual is the first annual review of the Scottish Version of The Caldicott Guardian Manual, which was first released in 2007 following the 2006 Department of Health publication ‘The Caldicott Guardian Manual 2006’.

### Objective

Best Practice Guidance

### Linked Documentation

UK Council Caldicott Guardians Manual 2006, is a DH publication, which provides guidance that takes into account of developments in information management in the NHS and in Councils with Social Services responsibilities since the publication of the Caldicott Report. It sets out the role of the Caldicott Guardian within an organisational Caldicott/confidentiality function as part of broader information governance.

### Document Sponsor

Scottish Government Health Directorate

### Approved by/Unapproved & Date

| **Author** | Information Governance team |
| **Contact Tel.** | 0131 275 6865 |

### Review Date

Annually, due for review July 2009

### Amendment History

<table>
<thead>
<tr>
<th><strong>Date</strong></th>
<th><strong>Issue No.</strong></th>
<th><strong>Section/Page</strong></th>
<th><strong>Details of Change</strong></th>
<th><strong>Authorised By:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Index

**Caldicott Guardian Manual for Scotland – 2008 Update**

- Introduction .......................................................... 3
- Who should be a Caldicott Guardian .......................... 4
- The Role of the Caldicott Guardian ............................. 5
- Information Governance .......................................... 7

**Appendices – Supplementary Guidance and Advice (Scotland Only)**

- Appendix I (Controlling Access) .............................. 9
- Appendix II (Summary of Scottish Government Health Directorate Publications) ................................................. 14
- Appendix III (Support and Advice for Guardians) ........ 21
1. Introduction

1.1 The 1997 report of the Review of Patient-Identifiable Information, chaired by Dame Fiona Caldicott (the Caldicott Report), made a number of recommendations for regulating the use and transfer of person identifiable information between NHS organisations in Scotland and to 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.

1.2 The recommendations of the Caldicott Committee defined 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” of person-based clinical information to oversee the arrangements for the use and sharing of clinical information. In Scotland these recommendations did not apply to Local Authorities, so Caldicott Guardians exist for NHS organisations only.

1.3 A key recommendation of the Caldicott Committee was that every use or flow of patient-identifiable information should be regularly justified and routinely tested against the principles developed in the Caldicott Report.

**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

1.4 Since then developments in information management in the NHS have added further dimension to the Caldicott role. These include:

- the Data Protection Act 1998
- the Human Rights Act 1998
- the Freedom of Information (Scotland) Act 2002
- Protecting Patient Confidentiality: NHSScotland Code of Practice
- NHS Information Governance 2005
- e-health developments (such as the Emergency Care Summary SCI Store, SCI DC etc)
- the election of the UK Caldicott Guardian Council 2005
1.5 This guidance 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 broader Information Governance. The guidance does not aim to reproduce or codify all the guidance available, but it updates existing materials where necessary and otherwise provides pointers to other current sources of guidance and standards. It supersedes the Caldicott Guardian manual published in 1999. This new Caldicott Guardian guidance will be reviewed annually and updated as required.

2. Who should be a Caldicott Guardian?

2.1 The Guardian should be, in order of priority:

- an existing member of the management board or senior management team of the organisation
- a senior health professional
- the person with responsibility for promoting clinical governance or equivalent functions within the organisation

2.2 Where it is not practicable to satisfy the criteria listed above, assignment of Guardian responsibility should be kept under review. The individual providing the role should also have a close relationship with the senior health professional responsible for promoting clinical governance or their social care equivalent.

2.3 It is particularly important that the Guardian has the seniority and clear authority from the Board / senior management team and Chief Executive to influence policy development and strategic planning, and carry the confidence of his or her colleagues. Obvious candidates for the role include:

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Possible Caldicott Guardian</th>
</tr>
</thead>
<tbody>
<tr>
<td>NHS Boards</td>
<td>Executive Board-level Director/Senior Health Professional</td>
</tr>
<tr>
<td>Cancer Registry</td>
<td>Senior officer - clinically qualified if possible</td>
</tr>
<tr>
<td>Clinical Research Bodies</td>
<td>Clinically qualified board member with ethics responsibilities</td>
</tr>
<tr>
<td>Non-NHS Clinical Contractor</td>
<td>Senior clinical manager</td>
</tr>
</tbody>
</table>

2.4 Individual general medical and dental practices, pharmacists and opticians do not need to appoint a Caldicott Guardian, but do need to have an Information Governance lead who, if they are not a clinician will need support from a clinically qualified individual. NHS Boards and Community Health Partnerships should ensure that within every practice there is an Information Governance lead who provides support and guidance as required.

2.5 Quantifying the time that should be allocated to Caldicott duties is difficult to do without a clear understanding of the context and available support for the Guardian. Examples of what has been found to work well or otherwise will be
3. The Role of the Caldicott Guardian

3.1 The Caldicott Guardian should play a key role in ensuring that NHS and partner organisations satisfy the highest practical standards for handling patient 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, Records Managers and IT Security staff contributing to the work as required.

3.2 The Caldicott Guardian also has a strategic role, however, that it is less appropriate to delegate. This involves representing and championing Information Governance requirements and issues at Board / management team level and, where appropriate, at a range of levels within the organisations overall governance framework.

3.3 Sample job descriptions and specifications can be accessed from www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott/caldressources/jobs/nhs.rtf
Table 2: Key Caldicott Responsibilities

<table>
<thead>
<tr>
<th>Strategy &amp; Governance</th>
<th>Confidentiality &amp; Data Protection expertise</th>
<th>Internal Information Processing</th>
<th>Information Sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td>the Caldicott Guardian should champion confidentiality issues at Board / management team level, should sit on an organisation’s Information Governance Board/Group and act as both the ‘conscience’ of the organisation and as an enabler for appropriate information sharing.</td>
<td>the Caldicott Guardian should develop a knowledge of confidentiality and data protection matters, drawing upon support staff working within an organisation’s Caldicott function but also on external sources of advice and guidance where available.</td>
<td>the Caldicott Guardian should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff. The key areas of work that need to be addressed by the organisation’s Caldicott function are detailed in the Information Governance Standards within the Information Governance Toolkit.</td>
<td>the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within and outside the NHS. This includes flows of information to and from partner agencies, sharing through NHS IT systems, disclosure to research interests and disclosure to other agencies e.g. the police.</td>
</tr>
</tbody>
</table>

4. Information Governance

4.1 Information Governance is a framework for handling all information in a confidential and secure manner to appropriate ethical and quality standards. NHS Information Governance\(^1\) is one element of the NHS Quality Improvement Scotland Clinical Governance and Risk Management standards. These standards will assist NHS Boards to develop and improve Information Governance locally. Information Governance has six main components:

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

4.2 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 the links provided in the guidance section of this document.

4.3 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

---

\(^1\)An introductory booklet describing NHSScotland Information Governance can be found at [http://www.elib.scot.nhs.uk/portal/ig/Pages/LinkThroughChecker.aspx?nid=99250](http://www.elib.scot.nhs.uk/portal/ig/Pages/LinkThroughChecker.aspx?nid=99250)
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.

4.4 The review of Information Governance in Scotland has led to the development of Information Governance Standards\(^2\) 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 attend the meetings.

4.5. The NHS Scotland Information Governance Electronic Toolkit is an online self-assessment tool that all NHS Scotland organisations are required to complete on a quarterly basis. The Toolkit enables NHS Boards/ Special Health Boards to record progress against National Information Governance Standards, which are an integral part of the NHS QIS Clinical Governance and Risk Management (CGRM) Standards.

The Information Governance Standards cover a number of key areas:
- Policy & Planning
- Confidentiality
- Freedom of Information
- Records Management – 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 Standard concerns Caldicott.

It is vital that the “Designated Director” for Information Governance has oversight of the submissions as they will utilised by NHS Quality Improvement Scotland to inform the Clinical Governance and Risk Management Peer Review Visits.

The Statement on Internal Control is part of the overall 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 the 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 and Information Governance Toolkit

\(^2\) [http://www.elib.scot.nhs.uk/portal/ig/Pages/LinkThroughChecker.aspx?nid=99244](http://www.elib.scot.nhs.uk/portal/ig/Pages/LinkThroughChecker.aspx?nid=99244)
APPENDIX I - CONTROLLING ACCESS

1. The Guardian as Gatekeeper

Once an organisation 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 new procedures can provide an opportunity to set high standards from the outset. This section provides an outline of key access control concepts and recommended good practice.

2. Access Control

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 about individuals;
- access to computer files and databases containing confidential information about individuals.

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 the Guardian be aware of current organisational capacity and intentions, through the management audit (see relevant section of this guidance). Detailed guidance on access controls can be found in the NHS Information Security Policy (see Appendix II - Support & Advice).

2.3. Specific access controls have been published for Scottish Care Information (SCI) Store Lab results [http://www.confidentiality.scot.nhs.uk/access_protocols.htm](http://www.confidentiality.scot.nhs.uk/access_protocols.htm) and for SCI Gateway [http://www.sci.scot.nhs.uk/products/gateway/gateway_prot_library.htm](http://www.sci.scot.nhs.uk/products/gateway/gateway_prot_library.htm)
3. Physical Access Controls

Physical security protection should be based on defined physical perimeters 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.

4. Access to Systems Utilities

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).

5. Access to Confidential Information about Individuals

5.1. 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

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

5.3. There are also legal restrictions on who may see certain patient-identifiable information. Only staff whose responsibilities include the treatment of individual patients with such diseases, or 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 the section on safe-havens below).

6. Information/Data “Ownership”

6.1. 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 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.

6.2. Details of the other responsibilities of “data owners” - e.g. data classification, security measures and compliance with Data Protection legislation - can be found within the NHSScotland Information Security Policy - NHS HDL (2006) 41.

7. Access Levels and Registration

7.1. 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.

7.2. 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.

7.3. 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).

8. 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 Chief Executive of NHS Board. Where appropriate, advice on the handling of such breaches of confidence should be sought from the Scottish Government Health Directorate.
9. Safe-Havens

9.1. 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.

9.2. 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.

9.3. 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.

9.4. Safe-haven arrangements originated to support contracting procedures, and detailed guidance was provided in MEL(92)42 (see Appendix III). 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.

9.5. Retention and disposal of information should be in line with the Scottish Government Health Department guidance contained within Annex D of the NHSScotland Records Management Code of Practice.

9.6. 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.
- 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
APPENDIX II - SUMMARY OF SCOTTISH GOVERNMENT HEALTH DIRECTORATE PUBLICATIONS

1. Introduction

Although there is considerable guidance available on different aspects of how the NHS should go about protecting and using confidential patient information, it is not always easy to locate the relevant guidance on a particular issue. This section of the manual provides an overview of The Scottish Government Health Directorate guidance and is intended as a navigation aid for Guardians. It is acknowledged however, that this is a complex and often controversial area; Guardians are therefore advised to seek advice on issues of uncertainty (see Appendix III).

2. Guidance

2.1. The Code of Practice on the Confidentiality of Personal Health Information

Issued under cover of NHS Circular No1990 (Gen) 22 provides guidance on the principles to be followed by all NHS staff in respect of personal health information. It reinforces the responsibilities of staff not to divulge information without the approval of the patient except in certain well defined circumstances. Copies of the Code can be obtained from:

Information Governance Programme
NHS National Services Scotland
Information Services Division
1 South Gyle Crescent
Edinburgh
EH12 9EB

Tel: 0131 275 6865

2.2. The NHS Information Security Policy

Issued in 2006 sets out the roles and responsibilities of different staff groups in relation to information security. It examines the role of senior management in setting objectives and developing an information strategy and looks at the elements of a supporting information security policy. Copies of this guidance are on the website http://www.security.scot.nhs.uk/ The website is accessible over the internet to NHS personnel or through user ID and password access over the internet.

The information security policy provides a clear operating framework for the organisation. Its key elements include:

- security management responsibilities,
- an assessment of threats and vulnerabilities,
- counter-measures adopted and security incident management procedures.
The guidance also provides detailed advice on a wide range of technical topics including:

- Assets Inventory
- Risk Analysis and Risk Assessment
- Secure Use of Passwords
- Equipment Security
- Access Control – including physical access, logical access, data ownership, user registration, and password control
- Security Incidents
- Virus Controls
- Business Continuity
- Housekeeping
- Security Monitoring

Further policy advice and guidance on Information Governance issues can be obtained from The Digital Information Policy branch of Connecting for Health. diginfo@dh.gsi.gov.uk

Additional information for general practitioners can be found in the SCIMP publication ‘Good Practice Guidelines for General Practice Electronic Patient Records’ http://www.scimp.scot.nhs.uk/gpg.html

Responsibility for the implementation of the information security policy rests with an identified and suitably qualified Information Security Officer.

2.3. NHS Mail – eHealth Clinical Communications


2.4. Joint inspection of children’s services HDL (2006) 35

This HDL provides information on the Joint Inspection of Children’s Services and Inspection of Social Work Services (Scotland) Act 2006, the code of practice for joint inspections under the Act and plans for joint inspections of child protection. The Code of Practice which accompanies this HDL sets out the role of the Caldicott Guardian.

2.5. Confidentiality and Disclosure of Information: General Medical Services (GMS), Section 17c Agreements, and Health Board Primary Medical Services (HBPMS) Code of Practice and Directions - PCA(M)(2005)10

This Code of Practice sets out guidance on the confidentiality of information held by those who provide General Medical Services (GMS), Section 17C Agreements and NHS Board Primary Medical Services (HBPMS). It also sets out guidance on the provision of contractor-held information to NHS Boards, and access by, and disclosure of, that information to NHS Boards or a person authorised in writing by NHS Boards: http://www.sehd.scot.nhs.uk/pca/PCA2005(M)10.pdf

2.6. Taking and using visual and audio images of patients

Video and audio recordings of treatment may be used both as a medical record or treatment aid in themselves, and as a tool for teaching, audit or research. The purpose and possible future use of the video and audio recordings must be clearly explained to individuals, before their consent is sought for the recording to be made. If recordings are to be used for teaching, audit or research, patients must be aware that they can refuse without their care being compromised and that when required or appropriate the recordings can be anonymised. As a matter of good practice, the same principles should be applied to clinical photography.

It is not intended that these legitimate recordings be curtailed in any way - context and the judgement of clinicians must remain paramount - but every care must be taken to ensure that guidelines on confidentiality are followed and that the informed consent of patients and medical staff is obtained where appropriate. Wherever possible, consent should be obtained in writing.

Further Guidance is available at:

http://www.gmc-uk.org/guidance/current/library/making_audiovisual.asp#11

General Medical Council - Good Practice in Prescribing Medicines (2006) – Remote prescribing via telephone, email, fax, video link or a website
http://www.gmc-uk.org/guidance/current/library/prescriptions_faqs.asp#p38

British Medical Association - Taking and using visual and audio images of patients (Oct 2007)
http://www.bma.org.uk/ap.nsf/AttachmentsByTitle/PDFAVRecordings/$FILE/Audio+and+visual+recordings.pdf

Cherri Pie - Clinical Recordings for Academic Non-clinical Settings
http://www.cherri.mvm.ed.ac.uk/
http://www.cherri.mvm.ed.ac.uk/cherri.pdf

Institute of Medical Illustrators
http://www.imi.org.uk/lawethics/law-ethics01.asp
2.7. Gold Standard Information Sharing Protocol

Information sharing protocol jointly commissioned by the Scottish Executive’s 21st Century Government Unit and the eCARE Programme.
### 3. Table of Scottish Government Health Directorate Circulars

<table>
<thead>
<tr>
<th>TITLE</th>
<th>LOCATION</th>
<th>POINTS TO NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCA (M)(2005) 10 Confidentiality and Disclosure of Information: General Medical Services (GMS), Section 17c Agreements, and Health Board Primary Medical Services (HBPMS) Code of Practice and Directions</td>
<td><a href="http://www.show.scot.nhs.uk/sehd/pca/PCA2005(M)10.pdf">http://www.show.scot.nhs.uk/sehd/pca/PCA2005(M)10.pdf</a></td>
<td>The Code of Practice sets out guidance on the confidentiality of information held by contractors who provide General Medical Services (GMS), Section 17c Agreements and Health Board Primary Medical Services (HBPMS).</td>
</tr>
<tr>
<td>Document</td>
<td>URL</td>
<td>Summary</td>
</tr>
<tr>
<td>----------</td>
<td>-----</td>
<td>---------</td>
</tr>
<tr>
<td>MEL (1997) 45 Guidance on use of fax for transfer of personal health information within NHSS</td>
<td><a href="http://www.show.scot.nhs.uk/sehd/mels/97_45.html">http://www.show.scot.nhs.uk/sehd/mels/97_45.html</a></td>
<td>Named data may only be sent by fax subject to strict conditions.</td>
</tr>
</tbody>
</table>

2 [http://www.confidentiality.scot.nhs.uk/publications/Draft%20040703%20REVISED%20HDL%20Clarification%20of%20HDL_1.doc](http://www.confidentiality.scot.nhs.uk/publications/Draft%20040703%20REVISED%20HDL%20Clarification%20of%20HDL_1.doc)
<table>
<thead>
<tr>
<th>Reference</th>
<th>URL</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOHHD No 1991(GEN)27 Access to Health Records Act 1990</td>
<td>[No web link available – plan to add scanned version to manual]</td>
<td>Advice to the service on AHR90- note this Act now only applies to access in relation to records of the deceased.</td>
</tr>
</tbody>
</table>
APPENDIX III - SUPPORT & ADVICE FOR GUARDIANS

1. Introduction

1.1. This manual aims to provide straightforward guidance on the key tasks that need to be addressed by the NHSScotland but beyond that, the intention is that it should serve as a resource for Guardians, identifying and summarising key guidance, flagging up sources of advice and highlighting training opportunities. It is also intended that the manual will be updated as new material becomes available.

1.2. An electronic copy of the Manual is available via the Information Governance e-Library. The Information Governance e-Library provides access to resources to support Caldicott Guardians across Scotland. It contains a range of materials relevant to Caldicott Guardians and those working within an organisations Caldicott function. It also provides tools to share resources, good practice and experience with colleagues via the Information Governance Knowledge Network.

http://www.elib.scot.nhs.uk/portal/ig/Pages/index.aspx

2. Information Governance Structures and Networking Opportunities

2.1. Guardians may wish to establish local networks either within NHS Board areas or more widely. These may productively be NHS Board based with all Community Health and Care Partnerships and NHS Boards being included.

2.2. Wider networking may also prove desirable, e.g. between NHS Boards and across NHS Board boundaries.

2.3. Networking will enable 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.

2.4. Examples of existing networking structures which may prove useful include:

- **Data Sharing Partnerships**

- **National Practice Forum**
  http://www.nationalpracticeforum.org/

- **NHSScotland National Information Governance Business Meetings**
  The meetings bring together the Health Records Manager Forum, NHS Data Protection Officers Forum and NHS Freedom of Information Forum). Email infogov@isd.csa.scot.nhs.uk for further details.

- **NHSScotland Information Security Forum**
  http://www.security.scot.nhs.uk/itsoforum.htm
• **NHS National Services Scotland Privacy Advisory Committee**

The Privacy Advisory Committee (PAC) was set up in the early ‘90’s to advise Information Services (ISD) and 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](http://www.isdscotland.org/isd/3048.html)

• **CHI Advisory Group**

CHI AG 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 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.

More information on the CHI Advisory Group can be found at: [http://www.chiadvisorygroup.scot.nhs.uk/](http://www.chiadvisorygroup.scot.nhs.uk/)

• **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.


3. **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. There are three elected members 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 web-site contains the minutes of Council meetings, back issues of the Caldicott Guardian newsletter, Frequently Asked Questions, example job descriptions and specifications and other useful information. These are available at:
http://www.connectingforhealth.nhs.uk/infogov/caldicott

An e-mail help line that is supported by Magi Nwolie, part of the Council secretariat. Magi will endeavour to find answers to questions and will collate responses as part of the Council’s FAQ resource caldicott.guardian@cfh.nhs.uk

4. Training for Caldicott Guardians

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

4.1. University of Bath Postgraduate Programme in Healthcare Information Governance

The School for Health, University of Bath has developed a postgraduate programme in Information Governance. Designed and developed by a multi-professional team, the programme will:

- Provide a comprehensive, innovative, practitioner-based approach to understanding issues around Information Governance in health and social care
- Meet the needs of those working in professional information roles, from clinical to managerial
- Equip graduates with the necessary skills and knowledge to undertake leadership roles in Information Governance within health and social care organisations
- Be delivered by distance learning – blending e-learning with face to face teaching

The Postgraduate programme in Healthcare Information Governance can be studied to CPD, Postgraduate Certificate, Postgraduate Diploma and MSc. Further information is available on the University of Bath website http://www.bath.ac.uk/health/hig/

4.2. 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 guidance for collection, storage and use of information in healthcare delivery
• 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.

The Postgraduate programme in Health care Information Governance can be studied to Postgraduate Certificate, Postgraduate Diploma and MSc. Further information is available on the University of Edinburgh website http://www.fhi.resed.ac.uk/site/2494/default.aspx

4.3. NHSScotland Data Protection and Confidentiality Package
This training package contains eight modules. The aim is to raise awareness of the rules and responsibilities when handling personal information outlining considerations in Data Protection, confidentiality and security that affect their daily work. The training package is available to all NHSScotland staff at http://www.datatraining.scot.nhs.uk

4.4. BMJ Learning
The BMJ online learning provides over 300 up to date learning resources for professionals in primary care and hospital medicine and offers a range of services to support medical 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

4.5. ISEB- Data Protection
Provides a recognised qualification at Certificate level for those with data protection responsibilities, as well as providing an effective conversion route for those needing to update their knowledge of and practice under the 1998 Data Protection Act. Further details are available at: http://www.bcs.org/server.php?show=nav.00101000200300f

4.6. Edinburgh Law School
The Centre offers a, "Law and Medical Ethics” Continuing Professional Development course delivered entirely online. The Programme includes a series of modules, which can be taken as a seven- or ten-week course, or as individual modules. 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/index.aspx

4.7. University of Glasgow - Masters in Medical Law (Distance Learning)
The Masters in Medical Law programme comprises study for two years, based around online distance learning modules, supplemented by attendance at residential weekends. The Programme has been running since 1998, focusing on contemporary medicolegal issues. It provides an opportunity to engage in topical and frequently controversial issues in medical law and ethics, within a flexible learning context. Modules include principles of consent and confidentiality.
Further information is available at: http://www.gla.ac.uk/departments/schooloflaw/postgraduatedegrees/medicallawprogrammes/

Or by contacting:
Dr C Gavaghan at C.Gavaghan@law.gla.ac.uk or Mrs G McGuire at G.McGuire@law.gla.ac.uk .
5. NHSScotland and National Sources of Advice for Guardians

5.1. List of Contacts by Subject Area

<table>
<thead>
<tr>
<th>Person/Organisation</th>
<th>Subjects Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Governance Policy Lead Scottish Government Health Directorate</td>
<td>• Information Governance Policy</td>
</tr>
<tr>
<td>St Andrew’s House</td>
<td></td>
</tr>
<tr>
<td>Edinburgh</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>NHSScotland Information Security Consultant</td>
<td>• IT Security</td>
</tr>
<tr>
<td>NHS National Services Scotland</td>
<td>• Information Security</td>
</tr>
<tr>
<td>National Information and Support Systems Group</td>
<td></td>
</tr>
<tr>
<td>Gyle Square</td>
<td></td>
</tr>
<tr>
<td>1 South Gyle Crescent</td>
<td></td>
</tr>
<tr>
<td>Edinburgh</td>
<td></td>
</tr>
<tr>
<td>EH12 9EB</td>
<td></td>
</tr>
<tr>
<td>Tel: 0131 275 6678</td>
<td></td>
</tr>
<tr>
<td>Website: <a href="http://www.security.scot.nhs.uk">http://www.security.scot.nhs.uk</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>NHSScotland Data Protection Adviser</td>
<td>• Data Protection</td>
</tr>
<tr>
<td>NHS National Services Scotland</td>
<td></td>
</tr>
<tr>
<td>Information Services Division</td>
<td></td>
</tr>
<tr>
<td>Gyle Square</td>
<td></td>
</tr>
<tr>
<td>1 South Gyle Crescent</td>
<td></td>
</tr>
<tr>
<td>Edinburgh</td>
<td></td>
</tr>
<tr>
<td>EH12 9EB</td>
<td></td>
</tr>
<tr>
<td>Tel: 0131 275 7176</td>
<td></td>
</tr>
<tr>
<td>Website: <a href="http://www.elib.scot.nhs.uk/portal//ig/Pages/index.aspx">http://www.elib.scot.nhs.uk/portal//ig/Pages/index.aspx</a></td>
<td></td>
</tr>
</tbody>
</table>
| Standards Branch                      | Policy on the sharing of personal data e.g. Gold Standard Data Sharing Policy  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Transformational Technologies Division</td>
<td>Development of national data standards</td>
</tr>
<tr>
<td>Scottish Government</td>
<td></td>
</tr>
<tr>
<td>Victoria Quay</td>
<td></td>
</tr>
<tr>
<td>Edinburgh</td>
<td></td>
</tr>
<tr>
<td>EH6 6QQ</td>
<td></td>
</tr>
<tr>
<td>Tel: 0131 244 4728</td>
<td></td>
</tr>
<tr>
<td>Website: <a href="http://www.scotland.gov.uk/Topics/Government/DataStandardsAndeCare">http://www.scotland.gov.uk/Topics/Government/DataStandardsAndeCare</a></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Central Legal Office</th>
<th>Contact NHS Board Legal Adviser for legal advice regarding legislation relating to Information Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>NHS National Services Scotland</td>
<td></td>
</tr>
<tr>
<td>Anderson House</td>
<td></td>
</tr>
<tr>
<td>Breadalbane</td>
<td></td>
</tr>
<tr>
<td>Bonnington Road</td>
<td></td>
</tr>
<tr>
<td>Edinburgh</td>
<td></td>
</tr>
<tr>
<td>EH6 5JR</td>
<td></td>
</tr>
<tr>
<td>Tel: 0131 275 7800</td>
<td></td>
</tr>
<tr>
<td>Website: <a href="http://www.clo.scot.nhs.uk/">http://www.clo.scot.nhs.uk/</a></td>
<td></td>
</tr>
</tbody>
</table>

| Mr K Macdonald                       | Data Protection Act.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Assistant Information Commissioner</td>
<td>Legal Guidance and Good Practice Notes</td>
</tr>
<tr>
<td>Scotland</td>
<td></td>
</tr>
<tr>
<td>The Information Commissioner’s Office</td>
<td></td>
</tr>
<tr>
<td>28 Thistle Street</td>
<td></td>
</tr>
<tr>
<td>Edinburgh</td>
<td></td>
</tr>
<tr>
<td>EH2 1EN</td>
<td></td>
</tr>
<tr>
<td>Website: <a href="http://www.ico.gov.uk/">http://www.ico.gov.uk/</a></td>
<td></td>
</tr>
<tr>
<td>Email: <a href="mailto:Scotland@ico.gsi.gov.uk">Scotland@ico.gsi.gov.uk</a></td>
<td></td>
</tr>
</tbody>
</table>
5.2. List of Professional Bodies

The bodies that regulate the activities of health professionals produce codes of practice and guidance on standards.

For Doctors:

The General Medical Council
1Regent’s Place, 350 Euston Road, London NW1 3JN.
http://www.gmc-uk.org/index.asp

For Nurses, Midwives and Health Visitors:

The Nursing and Midwifery Council
23 Portland Place
London, W1N 4JT
http://www.nmc-uk.org/aDefault.aspx

For Arts therapists, Biomedical scientists, Chiropodists/podiatrists, Clinical scientists, Dieticians, Occupational therapists, Operating department practitioners, Orthoptists, Paramedics, Physiotherapists, Prosthetists/orthotists, Radiographers, Speech and language therapists:

The Health Professions Council
Health Professions Council
Park House
184 Kennington Park Road
London SE11
http://www.hpc-uk.org/

For Dentists:

General Dental Council
37 Wimpole Street
London W1M 8DQ
http://www.gdc-uk.org/

For Opticians:

General Optical Council
41 Harley Street
London W1N 2DJ
http://www.optical.org/

For Pharmacists:

Royal Pharmaceutical Society of Great Britain
1 Lambeth High Street
London SE1 7JN
http://www.rpsgb.org.uk/