Department of Health

The Caldicott Guardian Manual 2010

UK Council of Caldicott Guardians

DH INFORMATION READER BOX

Policy	Estates
HR / Workforce	Performance
Management	**IM & T**
Planning	Finance
Clinical	Partnership Working

Document Purpose	Best Practice Guidance		
ROCR Ref:		**Gateway Ref:**	14043
Title	The Caldicott Guardian Manual 2010		
Author	DH/Digital Information Policy		
Publication Date	01 Mar 2010		
Target Audience	PCT CEs, NHS Trust CEs, SHA CEs, Care Trust CEs, Foundation Trust CEs , Directors of Adult SSs, Directors of Children's SSs		
Circulation List			
Description	The manual, which is a DH publication, is guidance that takes account of developments in information management in the NHS & in Councils with Social Care responsibilities since the puiblication of the Caldicott report. It sets out the role of the Caldicott Guardian within an organisational Caldicott/confidentiality function as a part of broader Information Governance.		
Cross Ref			
Superseded Docs	Caldicott Guardian Manual 2006		
Action Required	N/A		
Timing	**N/A**		
Contact Details	Ifeoma Nwolie Digital Info Policy DH Informatics Directorate Quarry House Leeds LS2 7UE 0113 397 4479 www.dh.gov.uk/policyandguidance www.connectingforhealth/infogov/resources/new-guidance		
For Recipient's Use			

Contents

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 England 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. Subsequent work extended the requirement to appoint Caldicott Guardians into Councils with Social Care Responsibilities [CSSRs].

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 and CSSRs have added further dimension to the Caldicott role. These include:

- the Data Protection Act 1998;
- the Human Rights Act 1998;
- the Freedom of Information Act 2000;
- the NHS Code of Practice on Confidentiality 2003;
- the inception of NHS Information Governance 2003;
- ICT strategic developments (such as the NHS Care Record, Electronic Social Care Records, and the Secondary Uses Service) 2005 onwards;
- the election of the UK Caldicott Guardian Council 2005;
- section 251 of the NHS Act 2006 (formerly section 60 of the Health and Social Care Act 2001);
- establishment of the National Information Governance Board (NIGB) for health and social care as a statutory body in 2008;
- the Ethics and Confidentiality Committee of the National Information Governance Board;
- the final report on data handling procedures in Government by the Cabinet Office June 2008;
- publication of the NHS Constitution in January 2009 (updated March 2010);
- NHS Care Record Guarantee for England published in 2005 (updated 2009);
- Social Care Record Guarantee for England 2009.

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 replaces the Caldicott Guardian manual published in 2006. The intention is that this new Caldicott Guardian guidance will be reviewed annually and updated as required. Where necessary, updates will be published on the Caldicott web pages at: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott

1.6 This Manual should be read alongside the e-learning module "The Role of the Caldicott Guardian: NHS and Social Care", which provides more detailed information on all aspects of the Caldicott Guardian role. The module is available at: http://www.connectingforhealth.nhs.uk/igtrainingtool

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 or social care 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 or Director of Adult Social Services and Director of Children's Services to influence policy development and strategic planning, and carry the confidence of his or her colleagues. Obvious candidates for the role include:

Table 1: Caldicott Guardians by organisation type

Organisation	Possible Caldicott Guardian
Strategic Health Authority	Regional Director of Public Health
NHS Provider Trust	Board-level clinician
Primary Care Trust	Board member with clinical governance responsibilities
Special Health Authorities (using/sharing patient data)	Board-level clinician or other senior officer
Cancer Registries	Senior officer – clinically qualified if possible
Clinical Research Bodies	Clinically qualified board member with ethics responsibilities
Non-NHS Clinical Contractor	Senior clinical manager
Social Care	Senior social care professional manager
Independent care providers	Medical Director

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 (sometimes referred to as a Caldicott lead) who, if they are not a clinician, will need support from a clinically qualified individual. Primary Care Trusts should ensure that within every practice there is an Information Governance lead and provide 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 posted on the UK Council of Caldicott Guardians web-site: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott

3. The Role of the Caldicott Guardian

3.1 The Caldicott Guardian should play a key role in ensuring that NHS, CSSRs 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, and advise 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.

3.2 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 etc, contributing to the work required.

3.3 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/ senior management team level and, where appropriate, at a range of levels within the organisation's overall governance framework. This role is particularly important in relation to the implementation of the National Programme for IT and the development of Electronic Social Care Records (ESCRs) and Common Assessment Frameworks.

3.4 Sample job descriptions and specifications can be accessed through the links provided in the guidance section of this document.

Table 2: Key Caldicott Responsibilities
Strategy & Governance: the Caldicott Guardian should champion confidentiality issues at Board/senior 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.
Confidentiality & Data Protection expertise: 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.
Internal Information Processing: 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 Toolkit.
Information Sharing: 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 and CSSRs. This includes flows of information to and from partner agencies, sharing through the NHS Care Records Service (NHS CRS) and related new IT systems, disclosure to research interests and disclosure to the police.

3.5 Staff should be advised to seek assistance from the Caldicott Guardian where necessary; typical examples of such situations are:

- a request from the police for access to patient information;
- requests from patients to delete their records;
- an actual or alleged breach of confidentiality.

4. Information Governance and the IG Assurance Framework

4.1 NHS Information Governance[1] is one element of the Integrated Governance framework promoted by the Department of Health in its Integrated Governance Handbook 2006[2]. Information Governance has four main components:

- Information Governance Management;
- Confidentiality and Data Protection Assurance;
- Information Security Assurance;
- 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 Assurance 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 Assurance, 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.

4.4 A review of NHS Information Governance in England[3], carried out at the end of 2005 and subsequently approved by Ministers, called for a strengthening of existing requirements for organisations to have Information Governance steering groups or boards as outlined in the Information Governance Toolkit. The Caldicott Guardian role needs to be strongly represented on this steering group and it is recommended that Caldicott Guardians attend in person.

---

1 An introductory booklet describing NHS Information Governance can be found at http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links

2 http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4128739

3 http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links

4.5 Following the high profile personal data losses reported by Government departments during 2007/08, the Cabinet Office published a data handling report[4] that required Government departments and their delivery arms (i.e. their agencies and any organisations they were responsible for) to improve data handling and information security by:

- implementing core measures to protect personal data and other information;
- creating a culture that properly values, protects and uses information;
- putting in place stronger accountability mechanisms; and
- ensuring there is stronger scrutiny of performance.

4.6 In response to Government directives, David Nicholson, the Chief Executive of the NHS, initiated an Information Governance Assurance Programme. The Programme was charged with producing an Information Governance Assurance Framework for the Department of Health's delivery arm (the NHS, adult social care and related care providers). There was recognition that the NHS was already providing some forms of assurance through its use of the Information Governance Toolkit (IGT) to carry out annual IG performance assessments. The IGT sets out a range of standards or controls that encompass the entire Information Governance agenda and form the basis for work programmes in NHS organisations to provide the required assurance that an organisation is performing at the required level. Since its introduction in 2003/4 the IGT has served to reduce the burden on NHS organisations by eliminating duplication of effort and reducing central reporting requirements whilst providing:

- a 'one-stop' shop for guidance and resource materials;
- a clear framework for assurance and controls;
- an on-line tool for efficient performance assessment and reporting.

Over the past few years the IGT has been further developed and now includes, amongst others, tailored assessment sets for social care, general practices and other independent contractors, prison health, DH arms' length bodies and commercial third parties.

4.7 The IG Assurance Framework builds on the work already in progress in the NHS and is comprised of a number of internal processes, organisational structures and external measures including:

- strengthening of the annual IG performance assessment standards;

4 http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links

- a requirement for all organisations within the Department's delivery arm to carry out annual IG performance assessments;
- mandatory IG training for all staff involved in handling personal data, with training taking place on induction and reinforced on an annual basis;
- documenting IG performance in Statements on Internal Control, which are scrutinised by the National Audit Office and through spot checks by the Information Commissioner;
- bringing IG assurance within the risk management regime with formal internal audits performed each year;
- independent assurance of IG performance through external audit; and monitoring by the Audit Commission, the Care Quality Commission and, for Foundation Trusts, by Monitor;
- oversight and scrutiny of IG performance by the National Information Governance Board for Health and Social Care (NIGB).

4.8 The Caldicott Guardian has a key role to play regarding the aspects of the Information Governance Assurance Framework that impact on confidentiality and data protection. For example, the Guardian should own and oversee the confidentiality and data protection assurance requirements within the IG Toolkit and should ensure that the annual IG performance assessments are carried out by operational staff members involved in the Caldicott function. The Caldicott Guardian should advise the Board/ senior management team or the Accounting Officer of any issues relating to confidentiality and data protection assurance so that they can be included within the Statement of Internal Control.

4.9 Caldicott Guardians need to play a strong role in ensuring that governance arrangements are in place and effective in their organisation, therefore in addition to attending (and perhaps Chairing) the Information Governance Steering Committee or equivalent forum, Guardians should ensure that confidentiality issues are regularly discussed and decisions are minuted at Board/senior management team meetings. Areas for discussion will include results/implications of internal and external audits relating to confidentiality and data protection assurance and options for improvement where necessary.

5. The relationship with the Senior Information Risk Owner

5.1 The Cabinet Office data handling report recognised that senior level ownership of information risk is a key factor in the appropriate management of personal information. This led to the establishment of the role of the Senior Information Risk Owner (SIRO), a board level executive with particular responsibility for information risk.

5.2 The SIRO role was mandated for the NHS in June 2008, and Councils were required to appoint a SIRO by Local Government Authority data handling guidelines published later that year. The SIRO has responsibility for understanding how the strategic business goals of the organisation may be impacted by any information risks. As part of the management of information risks, organisations are required to carry out work to identify their information assets and assign "ownership" for each asset to an Information Asset Owner (IAO). The IAO should be a senior member of staff who is accountable to the SIRO.

5.3 There are a number of differences between the roles of the Caldicott Guardian and the SIRO that suggest that they should normally remain distinct and separate; for example, the Caldicott Guardian's main focus is patient identifiable information whereas the SIRO is concerned with the risks to information systems generally. At the same time there is clearly a need to ensure that the Caldicott Guardian works closely with the SIRO (and any organisational Information Asset Owners – IAOs) and that the Guardian is consulted where appropriate when information risk reviews are conducted for assets which comprise or contain patient/service user information. Organisations should consider whether the Caldicott Guardian should 'sign-off' information risk reviews in these circumstances.

5.4 The Caldicott Guardian role:

- is advisory, and accountable for that advice;
- is the conscience of the organisation;
- provides a focal point for patient/service user confidentiality & information sharing issues;
- is concerned with the management of patient/service user information.

5.5 Whilst the Senior Information Risk Owner role:

- is accountable for IG processes within their organisation;
- fosters a culture for protecting and using data;
- provides a focal point for managing information risks and incidents;
- is concerned with the management of all information assets.

There is more information on the role of the SIRO including a job description at: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/risk/nhsinforiskmgt

6. The UK Council of Caldicott Guardians

6.1 The Council is an elected body made up of Caldicott Guardians from organisations involved in the provision of health and social care services in the United Kingdom. It was set up to facilitate the sharing of good confidentiality practice and the promotion of a national approach to confidentiality and information sharing.

6.2 The Council has a Constitution which contains the following terms of reference:

- to be the national body for Caldicott Guardians;
- to promote the roles and activities of Caldicott Guardians within the UK;
- 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.

6.3 The Council was formally set up in October 2005 and meets on a quarterly basis. Its work to date has encompassed a range of areas in accordance with its strategic work plan including:

- publishing resources for Caldicott Guardians, such as the Caldicott Guardian newsletter and the Caldicott Guardian website;
- providing advice and guidance to Caldicott Guardians and staff working in the information governance field;
- providing formal responses to consultations;
- providing an opinion on documents and materials concerned with confidentiality issues;
- endorsing documents and materials impacting on the role of the Caldicott Guardian, such as the Manuals of England, Scotland and Wales, training materials and job descriptions.

6.4 The Council has developed a Statement of Collaborative Working with the National Information Governance Board for Health and Social Care and works closely with the Information Governance Policy team in Department of Health Informatics.

6.5 There is more information about the Council and its work on its website: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott

7. Training for Caldicott Guardians

The Information Governance Training Tool

7.1 Developed by the Policy team at DH Informatics in conjunction with the UK Council of Caldicott Guardians and a third party supplier, the content of the tool was driven by the training needs analyses carried out in 2007 for Caldicott Guardians and IG leads and by the requirement for NHS organisations to provide IG assurances, including induction and mandatory IG training. The tool comprises a structured e-learning programme with Introductory, Foundation and Practitioner level modules covering all aspects of IG. Each module has a set of assessment questions enabling the user to obtain a certificate on successful completion.

7.2 The Training Tool contains a range of modules covering all aspects of IG, including a module titled The Role of the Caldicott Guardian: NHS and Social Care. This is a practitioner level module aimed at newly appointed Caldicott Guardians and those needing to know more about the role. It might also be useful to existing Guardians wanting a refresher course. The module has the following learning points:

- understand why the role should be allocated to a senior member of staff;
- be aware of the difference between the role of the Caldicott Guardian and the role of the Senior Information Risk Owner;
- appreciate how the role fits into the Information Governance Assurance Framework;
- understand the importance of the role to the protection of confidential patient and service user information;
- understand the importance of the role in relation to appropriately sharing patient and service user information;
- understand the relevance of the role to the National Programme for IT;
- understand some of the deliberations to be made in the decision making process;
- know where to access advice and support.

7.3 Access to the products within the Training Tool is via self-registration or guest account. Everyone having an NHS or government email account is automatically eligible to register. Email domains of specific organisations (e.g. independent care providers) will be considered for addition to the Tool; however, webmail accounts

(e.g. Hotmail/Yahoo mail etc) are specifically excluded. An online registration process is also available for those who do not have an email address. Guest accounts require no login, but neither will they retain a record of the modules undertaken. To use the Tool, please visit: www.connectingforhealth.nhs.uk/igtrainingtool

ISEB Certificate in Data Protection

7.4 This qualification has been developed to provide candidates with an industry recognised qualification that incorporates the latest changes and updates outlined in the Data Protection Act of 1998. The qualification is aimed at those practitioners working with, or responsible for data protection. Further information about the Certificate in Data Protection can be obtained from the accredited Training Providers at: http://www.bcs.org/server.php?show=nav.7272

8. Guidance and links

General advice and support

The UK Council of Caldicott Guardians
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott

This 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. The Council can be contacted via the Secretariat at: ukccgsecretariat@nhs.net

The Secretariat will endeavour to find answers to questions and will collate responses as part of the Council's FAQ resource.

DH Informatics Directorate: Information Governance Policy
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov

The Information Governance Policy Branch provides policy advice and guidance on Information Governance issues and can be contacted via the Helpdesk by email at exeter.helpdesk@nhs.net or by phone on 01392 251289.

General Medical Council
http://www.gmc-uk.org/about/contacts

The General Medical Council provides assistance with standards and ethics enquiries and can be contacted by email at standards@gmc-uk.org or by phone on 0202 7189 5404.

The Information Governance Toolkit
www.igt.connectingforhealth.nhs.uk or nww.igt.connectingforhealth.nhs.uk

The IGT provides guidance on how organisations should satisfy confidentiality, data protection, information security, FOI, records management and information quality requirements. It also contains an extensive knowledgebase of exemplar documents, guidance materials and useful links. For assistance with the Information Governance Toolkit – content, technical advice and administration issues contact the Helpdesk by email at exeter.helpdesk@nhs.net or by phone on 01392 251289.

The National Information Governance Board for Health and Social Care (NIGB)
http://www.nigb.nhs.uk

The NIGB provides leadership and promotes consistent standards for information governance across health and social care. The Board considers ethical issues; the interpretation and application of the law and policies and provides advice on information governance matters at a national level via email at nigb@nhs.net or by phone on 0207 633 7052.

NIGB: The Ethics and Confidentiality Committee
http://www.nigb.nhs.uk/ecc

The Ethics and Confidentiality Committee (ECC) has been established to undertake the responsibilities of the NIGB under section 251 of the NHS Act 2006 (formerly section 60 of the Health & Social Care Act 2001) and to consider and advise on ethical issues relating to the processing of health or social care information as referred to it by the NIGB.

Nursing and Midwifery Council
http://www.nmc-uk.org/

The Nursing & Midwifery Council provides professional advice by email at advice@nmc-uk.org or by phone on 020 7333 9333

The Caldicott Guardian web pages
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott/caldresources

Information and resources for the Caldicott community, including guidance manuals, job descriptions and frequently asked questions.

The Department of Health
http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/index.htm

The DH website contains a range of materials relevant to Caldicott Guardians and those working within an organisation's Caldicott function.

Guidance on Information Sharing and legal aspects

Confidentiality NHS Code of Practice
http://www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf

Guidance on how confidentiality, data protection and human rights legislation impact on the use and sharing of patient information.

Data Sharing and Protection
http://www.justice.gov.uk/guidance/datasharing.htm

Guidance from the Ministry of Justice for professionals and practitioners on application of the Data Protection Act 1998.

HM Government Information Sharing Guidance
http://www.dcsf.gov.uk/everychildmatters/resources-and-practice/IG00340/

Cross Government information sharing guidance led by the Department for Children, Schools and Families for frontline practitioners that have to make information sharing decisions whilst working with adults and families and/or with children and young people. Resource materials can also be obtained from these web pages.

Data Protection Act 1998: Legal Guidance
http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx

Guidance produced by the Information Commissioner to explain how this fairly complex piece of legislation should be interpreted.

NHS Information Governance: Guidance on Legal and Professional Obligations
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links

Best practice guidance that outlines the likely impact on health and social care information, of the range of complex legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, those that permit or require information to be used or disclosed.

Mental Capacity Act 2005
http://www.dh.gov.uk/en/SocialCare/Deliveringadultsocialcare/MentalCapacity/MentalCapacityAct2005/index.htm

This website contains a range of information and guidance documents about the Mental Capacity Act 2005 (MCA). The materials include links to the MCA Code of Practice, guidance on consent related issues and training materials

Other Useful Guidance and/or Links

Guidance on good practice in information security
http://nww.connectingforhealth.nhs.uk/infrasec/gp **(NHSnet only)**

NHS CFH produces good practice guidelines on technical information security as well as the new controls that are being introduced in support of the NHS Care Records Service.

Records Management NHS Code of Practice & Roadmap
http://www.dh.gov.uk?PolicyAndGuidance/OrganisationPolicy/RecordsManagement

Guidance that replaces the previous records management circular, including records management principles, retention schedules and a legal compendium. The road map that accompanies the Code of Practice is an evolving body of guidance and best practice materials on specific aspects of records management and information quality.

Good Practice Guidelines for General Practice Electronic Records v3.1 (2005)
http://www.dh.gov.uk/PublicationsAndStatisticsPublications/PublicationsPolicyAndGuidance

Useful compendium of materials associated with paperless practice.

Cabinet Office Information Security and Assurance
http://www.cabinetoffice.gov.uk/csia.aspx

Further information related to the data handling review carried out in 2007/2008

The Information Governance Assurance Programme and Framework
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igap

Further information about the Programme set up to look at the Cabinet Office minimum standards for data handling, to review what the NHS was already doing, to identify gaps and put measures in place to fill the gaps.

NHS Information Risk Management
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/risk/nhsinforiskmgt

Guidance aimed at those responsible for managing information risk within NHS organisations.

© Crown copyright 2010
301463 1p 5k Mar 10
Produced by COI for the Department of Health

If you require further copies of this title visit
www.orderline.dh.gov.uk and quote:
301463 *The Caldicott Guardian Manual 2010*

Tel: 0300 123 1002
Minicom: 0300 123 1003
(8am to 6pm, Monday to Friday)

www.dh.gov.uk/publications