Department of Health

Information Security Management:

NHS Code of Practice

April 2007

Information Security Management:

NHS Code of Practice

April 2007

DH INFORMATION READER BOX

Policy HR/Workforce Management Planning Capital	Estates Performance **IM&T** Finance Partnership Working
Document purpose	Best practice guidance
Gateway reference	7974
Title	Information Security Management: NHS Code of Practice
Author	DH/Digital Information Policy
Publication date	April 2007
Target audience	PCT CEs, NHS Trust CEs, SHA CEs, Care Trust CEs, Foundation Trust CEs, Medical Directors, PCT PEC Chairs, NHS Trust Board Chairs, Special HA CEs, Directors of HR, Directors of Finance, Allied Health Professionals, GPs, Royal Colleges, BMA, GMC, Healthcare Commission, Monitor
Circulation list	
Description	The Code of Practice is a guide to the required methods and standards of practice in the management of information security. It will benefit all types of NHS organisations through the promotion and adoption of best practice.
Cross-reference	HSG(96)15: NHS Information Management and Technology Security Manual
Superseded documents	HSG(96)15: NHS Information Management and Technology Security Manual
Action required	N/A
Timing	N/A
Contact details	Adam Goodwin Digital Information Policy NHS Connecting for Health adam.goodwin@dh.gsi.gov.uk 0113 397 4495 NHSInformationSecurity@dh.gsi.gov.uk
For recipient's use	

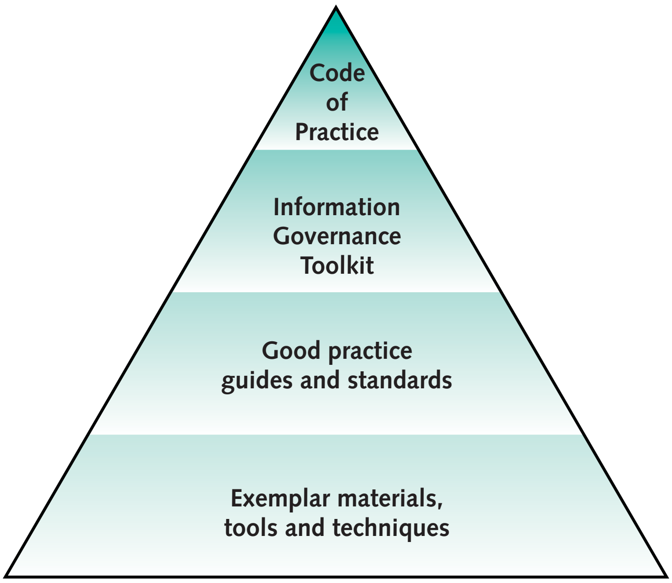
Contents

Section 1 – Foreword

1. Information Security Management: NHS Code of Practice has been published by the Department of Health as a guide to the methods and required standards of practice in the management of information security for those who work within, under contract to, or in business partnership with NHS organisations in England. Its purpose is to identify and address security management in the processing and use of NHS information and is based on current legal requirements, relevant standards and professional best practice.

2. The guidance was prepared by a working group made up of representatives from the Department of Health, NHS Connecting for Health, NHS Trusts, Strategic Health Authorities, GP practices and professional bodies. It has also been endorsed by interested stakeholders who were consulted on the draft document and their comments were incorporated into the final Code of Practice as appropriate.

3. The Code provides a key component of Information Governance arrangements for the NHS. This document is part of an evolving information security management framework because risk factors, standards and best practice covered by the Code will change over time. It, and other related materials, will therefore be subject to regular review and be updated as necessary.


Code of Practice
Information Governance Toolkit
Good practice guides and standards
Exemplar materials, tools and techniques

The NHS Information Security Management Framework

Types of Information Covered by the Code of Practice

4. The guidance contained within this Code of Practice and its related materials applies to NHS information assets of all types (including the records of NHS patients treated on behalf of the NHS in the private healthcare sector).

5. These information assets may consist of:

   - digital or hard copy patient health records (including those concerning all specialties and GP medical records);
   - digital or hard copy administrative information (including, for example, personnel, estates, corporate planning, supplies ordering, financial and accounting records);
   - digital or printed X-rays, photographs, slides and imaging reports, outputs and images;
   - digital media (including, for example, data tapes, CD-ROMs, DVDs, USB disc drives, removable memory sticks, and other internal and external media compatible with NHS information systems);
   - computerised records, including those that are processed in networked, mobile or standalone systems;
   - email, text and other message types.

Types of Organisation Covered by the Code of Practice

6. The guidance within this Code of Practice is generally applicable to all organisations that access or process NHS information of the types outlined above. This scope includes, but is not limited to, NHS organisations, third party IT/information service providers and private sector care providers providing care services under NHS contracts.

Section 2 – Introduction

7. This Code of Practice is a key component of the information security management framework that replaces prior Information Management and Technology security guidance published by the NHS Executive Information Management Centre and the NHS Information Authority, including *HSG(96)15: NHS Information Management and Technology Security Manual.*

8. The guidelines contained in this Code of Practice draw on advice and published guidance available from UK Government security authorities, the British Standards Institute, the Information Security Forum, and from best information security management practices followed by a wide range of organisations in the Government, public and private sectors. The guidelines provide a framework for consistent and effective information security management that is both risk and standards-based and is fully integrated with other key NHS Information Governance areas.

9. NHS managers need to be able to demonstrate positive progress in enabling their staff to conform to the guidelines, identifying resource requirements and any related areas where organisation or system improvements are required. Information Governance performance assessment and management arrangements facilitate and drive forward the necessary changes that enable improvement. Those responsible for monitoring NHS performance, for example Strategic Health Authorities and the Healthcare Commission, play a key role in ensuring that effective Information Governance systems are in place.

10. The NHS will be supported in delivering improved information security through the NHS Information Governance Toolkit (IGT). An information security management roadmap will be developed and published separately and incorporated within the IGT to support implementation of this Code of Practice.

General Context

11. NHS organisations need robust information security management arrangements for the protection of their patient records and key information services, to meet the statutory requirements set out within the Data Protection Act 1998 and to satisfy their obligations under the Civil Contingencies Act 2004. These aims are also consistent with the UK Strategy for Information Assurance published by the Cabinet Office (available at www.cabinetoffice.gov.uk/csia/documents/pdf/CSIA_booklet.pdf).

12. Without effective security, NHS information assets may become unreliable and untrustworthy, may not be accessible where or when needed, or may be compromised by unauthorised third parties. All NHS organisations and those who supply or make use of NHS information therefore have an obligation to ensure that there is adequate provision for the security management of the information resources that they own, control or use.

13. Information, whether in paper or digital form, is the lifeblood of NHS organisations because of its critical importance to NHS patient care and other related business processes. High-quality information underpins the delivery of high-quality evidence-based healthcare and many other key service deliverables. Information has greatest value when it is accurate, up to date and is accessible where and when it is needed. Inaccurate, outdated or inaccessible information that is the result of one or more information security weaknesses can quickly disrupt or devalue mission critical processes, and these factors should be fully considered when commissioning, designing or implementing new systems. An effective information security management regime, therefore, ensures that information is properly protected and is reliably available. NHS information may be needed to:

- support patient care and continuity of care;
- support day-to-day business processes that underpin the delivery of care;
- support evidence-based clinical practice;
- support public health promotion and communicate emergency guidance;
- support sound administrative and managerial decision making, as part of the knowledge base for the NHS;
- meet legal requirements, including requests from patients under the provisions of the Data Protection Act or the Freedom of Information Act;
- assist clinical or other types of audit;
- support improvements in clinical effectiveness through research;

- support archival functions by taking account of the historical importance of information;
- support patient choice and control over treatment and services designed around patients.

14. Information Security Management: NHS Code of Practice, together with its supporting annexes and other related guidance materials within the NHS IGT, identifies the actions, managerial responsibilities and baseline information security management measures applicable to all types of NHS information (i.e. both corporate and health).

Monitoring Information Security Management Performance

15. A number of bodies monitor NHS performance and, through their existing arrangements, have an interest in NHS information security management. The Healthcare Commission monitors a core governance standard relating to broad records management as part of its annual assessment of performance. The Audit Commission regularly conducts studies into information security management and related Information Governance issues. The Department of Health collects performance details as part of the annual Information Governance assessment, and these will inform the work of both the Healthcare Commission and the Audit Commission. The NHS Litigation Authority also assesses risk management arrangements through its NHSLA/CNST standards.

16. Other bodies likely to have interest or that may comment on Information Security Management performance may, for example, include the Health Service Ombudsman when investigating a complaint, and the Information Commissioner when investigating alleged breaches of Data Protection or Freedom of Information legislation. In addition, the Cabinet Office monitor and co-ordinate relevant information assurance initiatives within government and the wider public sector that enable trusted cross-boundary working and ensure protection of the UK Critical National Infrastructure.

Legal and Professional Obligations

17. The key statutory requirement for NHS compliance with information security management principles is the Data Protection Act 1998, and in particular its seventh principle. The Act provides a broad framework of general standards that have to be met and considered in conjunction with other legal obligations. The Act regulates the processing of personal data, held both manually and on computer. It applies to personal information generally, not just to health records, and therefore the same

principles apply to records of employees held by employers, for example in finance, human resources and occupational health departments.

18. Other applicable legislation relating to information and the information security management function shall be contained within additional guidance to be provided under separate cover and that shall relate to the NHS Information Governance function generally. Additionally, clinicians are under a duty to meet information security management standards set by their professional regulatory bodies.

NHS Connecting for Health (NHS CFH)

19. The impact of the Government's health reform and transformational government agenda will fundamentally affect the way the NHS approaches the management of all electronic records. The NHS Care Records Service (NHS CRS) and the establishment of Care Trusts are central to these reforms and will transform the way both health and social care information are managed. NHS CFH is working with a wide range of NHS organisations and professional bodies to ensure that all NHS patient records may be kept in electronic format in the future.

20. In the mixed economy of paper and electronic records that will exist as the NHS CRS is developed and implemented, it is essential that both paper and electronic records are managed securely and consistently to ensure that a complete health record is available at the point of need. This transitional period, during which the overall balance of paper and electronic records will change, will generate significant information security management challenges – for example before patient data is migrated to the national data spine and is securely accessible from there.

Social Care Information

21. Local authorities have responsibility for commissioning social care services. Increasingly, joint commissioning will take place between NHS organisations and local authorities. Recent policy developments, including the White Paper *Our Health, Our Care, Our Say*, highlight the need for health and social care to work together to provide seamless services to patients wherever the need arises. This has important implications for sharing information between health and social care. NHS organisations will increasingly need to seek assurance that their social care partners apply equivalent information security standards to their own and vice versa. Where cross-boundary NHS information sharing arrangements are required, the implementation of relevant and consistent standards for information security management provides the basis that underpins trust and confidence in those partnership arrangements.

NHS Information Governance: Information Security Policy

22. The purpose of the NHS Information Governance: Information Security Policy is to protect, to a consistently high standard, all information assets, including patient records and other NHS corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental.

23. This policy, correctly applied and adhered to, will achieve a comprehensive and consistent approach to the security management of information throughout the NHS, ensure continuous business capability, and minimise both the likelihood of occurrence and the impacts of any information security incidents.

24. It is the policy of the Department of Health that:

- a comprehensive, systematic and reliable programme for NHS information security management be established and maintained, based upon the principles identified within this Code of Practice and as may be periodically updated. This programme shall benefit NHS organisations of all types by establishing and maintaining a consistent and credible framework for secure information services of all types and at all levels. It is applicable to NHS organisations, their information services contractors and other business partner organisations of all types that access or use NHS information;
- threats to NHS data shall be appropriately identified and based upon robust risk assessment and management arrangements, and shall be managed and regularly reviewed to ensure:
  - protection against its unauthorised access or disclosure;
  - that the integrity and evidential value of information shall be maintained;
  - that information shall be available to properly authorised personnel as and when it is required;
- relevant regulatory and legislative requirements shall be achieved;
- NHS organisations shall have in place organisation-wide business continuity plans for their information systems. These should include the identification and assessment of critical dependencies on NHS information resources so that alternative fallback arrangements may be identified and tested, ensuring availability where necessary;
- relevant information security training and awareness will be available to all staff;

- all breaches of information security, actual or suspected, shall be recorded, reported to and investigated by an appropriately experienced and skilled Information Security Officer;
- all organisations that use NHS network infrastructure or digital services provided under a national contract shall satisfy and maintain the NHS information governance conditions for their provision;
- adequate audit provision, based upon robust risk management arrangements, shall be made to ensure the continuing effectiveness of NHS information security management arrangements;
- annual reporting of attainment be provided through the NHS IGT for all participating organisations.

25. A comprehensive NHS information security management framework is in place to support this policy. This framework takes the form of this Information Security Management: NHS Code of Practice supported through other relevant standards, methods and best practice guideline documents on a range of key information security aspects. These components shall be reviewed and may be updated and added to as threats, information technologies and best practice change.

Section 3 – NHS Information Security Management

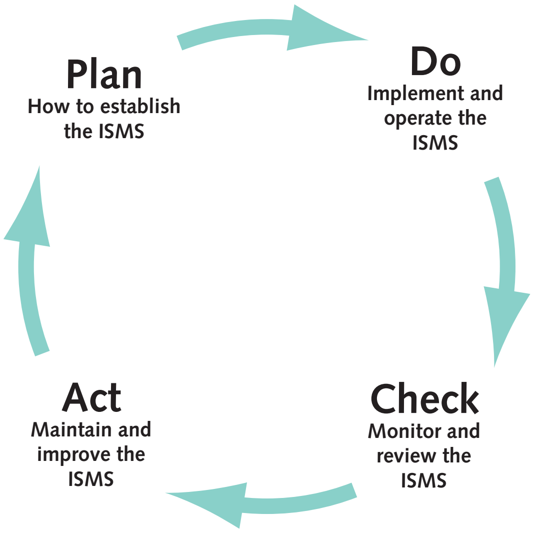
26. Information Security Management: NHS Code of Practice provides the basis for reliable and effective information security management by NHS organisations and is equally applicable to those organisations that may share in NHS information resources of all kinds. It shall be supplemented through a consistent and dynamic range of further guidance, methods, checklists and tools to be developed and that will be applicable to specific information security topics or practices. This Code of Practice is an integral component within the overall NHS Information Governance Programme.

Information Security Management System (ISMS)

27. Compliance with information security standards are normally measured through an organisation's Information Security Management System (ISMS) or equivalent. This is a documented model for establishing, implementing, operating, monitoring and improving the effectiveness of information security management within the organisation. For the NHS, the NHS IGT provides the basis of an ISMS that supports a basic but acceptable level of information security. For those organisations with special or advanced information security needs, the ISMS ensures a flexible approach that may be expanded in scope and content over time.

28. Effective information security involves more than simply installing a security product, implementing anti-malware software, providing a security policy or signing a contract with a support service provider. The ISMS therefore provides a means to identify and co-ordinate the approach to the management of information security by the organisation in order to protect it and its business partners.

29. An ISMS should also identify the chosen evaluation method and documentation processes that are relevant to the needs of the organisation. These provide the underlying principles of the Plan-Do-Check-Act (PDCA) model described within the ISO/IEC 17799:2005 standard that closely resembles the model for quality management (ISO 9001). Again, the NHS IGT provides the basis for implementing this model.


Plan
How to establish the ISMS
Do
Implement and operate the ISMS
Check
Monitor and review the ISMS
Act
Maintain and improve the ISMS

30. Core elements of an effective ISMS can be summarised as follows:

PLAN

Establishing the ISMS

- Define the business needs for information security and set these out within a corporate information security policy.
- Identify and assess the risks to information security.
- Either identify controls to be established to manage the information security risks identified, transfer the risks or accept them as appropriate, based on business needs and the risk appetite of the organisation.

DO

Implementing and operating the ISMS

- Develop and implement action plans to manage the identified information security risks.
- Implement training and awareness for all relevant staff.

CHECK

Monitoring and reviewing the ISMS

- Establish processes to identify actual and potential information security incidents or systems weaknesses.
- Monitor and update information security risk assessments as required.
- Monitor the effectiveness of the ISMS in managing information risks through internal reviews and independent audit.

ACT

Maintaining the ISMS

- Review and update the ISMS as required.

NHS Organisational Responsibility

31. Responsibility for information security management must be allocated appropriately within every organisation. There needs to be a clear managerial focus for the security of information of all types, in all formats (including electronic records), throughout their life cycle, from planning and creation through to ultimate disposal or destruction. Those individuals involved in this aspect of information governance should have clearly defined responsibilities and objectives, and access to adequate resources to achieve them.

32. Responsibility for information security resides, ultimately, with an organisation's Chief Executive, senior partners or equivalent responsible officers. This responsibility should be discharged through a designated member of staff who has lead responsibility for information security management within the organisation. The information security lead should be of appropriate seniority (e.g. Board level, or reporting directly to a Board member in a large organisation). This lead role should be formally acknowledged and made widely known throughout the organisation.

33. It is essential that the manager, or managers, responsible for information security management should work in close association with the manager or managers responsible for freedom of information, data protection, patient confidentiality and other information governance work areas. In smaller organisations it clearly makes sense for these responsibilities to rest with one or two appropriately placed individuals (e.g. a practice manager of a GP practice).

34. All staff, whether clinical or administrative, must be appropriately trained so that they are fully aware of their personal responsibilities in respect of information security, and that they are competent to carry out their designated duties. This should include training for staff in the use and protection of both paper and electronic records systems. Training requirements, including those for information governance specialists, should be regularly assessed and refreshed in order that staff may remain appropriately skilled/knowledgeable over time. Training must be supported by ensuring that staff have ready access to organisational policies, procedures and guidance documents and know where to go for advice when needed.

35. Training will need to be role specific, with staff responsible for information security management requiring in depth professional training and access to expert advice on relevant aspects of information governance. Within a smaller organisation, such as a GP practice, considerable support and advice may need to be provided by the appropriate Primary Care Trust. Organisations need to ensure that their staff are aware of all expected best practices, including having a demonstrable understanding of:

- what information they are using, how it should be used and how it should be protectively handled, stored and transferred, including outputs from computer systems;
- what procedures, standards and protocols exist for the sharing of information with relevant others and on a 'need to know' basis;
- how to report a suspected or actual breach of information security within the organisation, to an affected external information service provider or to a partner organisation.

Individual Responsibility

36. All individuals who work within, or under contract to, an NHS organisation have a general responsibility for the security of information that they create or use in the performance of their duties. For example, security expectations may be described within any or combinations of contracts of employment, consultancy or service contract, honourary contracts, professional codes of practice, information service user registration and set-up procedures, acceptable usage policies or other conditions of service that apply to either local systems or nationally provided services.

37. These expectations may also include the reporting of any suspected or known breaches of information security, or identified weaknesses within information systems they may use, to the organisation's nominated information security manager or relevant equivalent for consideration.

Information Security Policy (NHS Organisations)

38. Each NHS organisation should have in place its overall information security policy statement defining how it manages the security of its information assets, including its electronic records. The organisation's information security policy should be endorsed by the Board, senior partners, or responsible officers, and made readily available to all staff at all levels of the organisation, both on induction and through regular update training.

39. The information security policy statement should provide a mandate for robust and effective information security management. In particular, it should set out the organisation's commitment to create, maintain and manage the security of its key information assets and other external information resources that it may depend upon, and document its principal activities in this respect.

40. The policy should also:

- outline the role of information security management within the organisation, and its relationship to the organisation's overall information governance strategy;
- define information security management roles and responsibilities within the organisation, including the responsibilities of specialist staff or others who work under contract to the organisation, to document their security considerations and decisions for audit purposes;
- define the relationships and information security management roles and responsibilities within other organisations to which information services are provided or from which information services are received. This is an essential feature for the maintenance of relevant trust and confidence between information service partner organisations;
- provide a framework for all relevant supporting information security management standards, best practice procedures and guidelines;
- indicate the way in which compliance with the policy and its supporting standards, best practice procedures and guidelines will be monitored and maintained.

41. The information security policy statement should be reviewed at regular intervals, in line with the organisation's policy review requirements, and, if appropriate, it should be amended to maintain its scope, currency and relevance.

Information Risk Assessment

42. Effective information security management is based upon the core principle of risk assessment and management. This requires the identification and quantification of information security risks in terms of their perceived severity of impact and the likelihood of occurrence.

43. Once identified, information security risks need to be managed on a formal basis. Risks should be recorded within a risk register and action plans should be in place to demonstrate effective management of the risks. The risk register and all associated actions should be reviewed at regular intervals.

44. Regular reviews of implemented information security arrangements are an essential feature of an organisation's risk management programme. These reviews will help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed. The frequency and scope of local security reviews should be based upon the requirements for assurance as set out within the organisation's security policy and ISMS.

Annex A – Glossary of Terms

- **Asset**
  Anything that has value to the organisation, its business operations and its continuity.

- **Authentication**
  Ensuring that the identity of a subject or resource is the one claimed.

- **Availability**
  The property of being accessible and usable upon demand by an authorised entity.

- **BS7799-1**
  The original British Standard detailing the Code of Practice for Information Security Management, superseded by ISO/IEC 17799:2005.

- **BS7799-2:2002**
  The specification for information security management, superseded by ISO/IEC 27001:2005.

- **Business impact**
  The result of an information security incident on business functions and the effect that a business interruption might have upon them.

- **Confidentiality**
  The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

- **Impact**
  The result of an information security incident, caused by a threat, which affects assets.

- **Information Assurance**
  The confidence that information assets will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

- **Information Security**
  The preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

- **Information Security Management System (ISMS)**
  That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

- **Integrity**
  The property of safeguarding the accuracy and completeness of assets.

- **ISO/IEC 17799:2005**
  The current international Code of Practice for Information Security Management (superseded BS7799-1). Is scheduled to become ISO/IEC 27002 in a few years' time. Closely aligned with ISO/IEC 27001:2005.

- **ISO/IEC 27001:2005**
  The current international specification for the ISMS (superseded BS7799-2:2002). Closely aligned with ISO/IEC 17799:2005.

- **Mitigation**
  Limitation of the negative consequence of a particular event.

- **Non-repudiation**
  The ability to prove an action or event has taken place, so that this action or event cannot be repudiated later.

- **Residual Risk**
  The risk remaining after risk treatment.

- **Risk**
  The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.

- **Risk Acceptance**
  The decision to accept a risk.

- **Risk Analysis**
  The systematic use of information to identify sources and to estimate the risk.

- **Risk Appetite**
  The attitude taken by an organisation, which, in relation to risk, minimises the negative and maximises the positive business consequences and their respective probabilities.

- **Risk Assessment**
  The overall process of risk analysis and risk evaluation.

- **Risk Avoidance**
  The decision not to be involved in, or action to withdraw from, a risk situation.

- **Risk Evaluation**
  The process of comparing the estimated risk against given risk criteria to determine the significance of risk.

- **Risk Identification**
  The process to find, list and characterise elements of risk.

- **Risk Management**
  The process of co-ordinating activities to direct and control an organisation with regard to risk.

- **Risk Management System**
  The set of elements of an organisation's management system concerned with managing risk.

- **Risk Reduction**
  The action taken to lessen the probability, negative consequences, or both, associated with risk.

- **Risk Retention**
  The acceptance of the burden of loss, or benefit of gain, from a particular risk.

- **Risk Transfer**
  Sharing with another party the burden of loss or benefit of gain for a risk.

- **Risk Treatment**
  The process of selection and implementation of measures to modify risk.

- **Statement of Applicability**
  A document describing the control objectives and controls that are relevant and applicable to the organisation's ISMS, based on the results and conclusions of the risk assessment and risk treatment processes.

- **Threat**
  A potential cause of an incident that may result in harm to a system or organisation.

- **Vulnerability**
  A weakness of an asset or group of assets that can be exploited by one or more threats.

Annex B – Resources to Support Improvement

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

Information governance is defined as:

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

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

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

The information governance framework addresses a number of different aspects of NHS information handling over a number of key work areas, i.e. the Caldicott recommendations on the use of patient identifiable information, the Confidentiality Code of Practice, the Data Protection Act 1998, the Freedom of Information Act 2000, Information Management and Technology Security (BS7799/ISO 17799, Code of Practice for Information Security Management), Health Records Management, Corporate Records Management and Information Quality Assurance. It provides a vehicle to develop clear standards and directly link the standards to support and guidance materials and exemplar documentation.

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

The IGT provides the means by which NHS organisations can assess their compliance with current legislation, government policy and national guidance. It has been approved by Health Ministers and the Review of Central Requirements Committee.

The Healthcare Commission also uses the IGT as part of the standard to audit NHS organisations against the new core standards, as set out in its *Criteria for Assessing Core Standards.*

The information governance framework details the standards expected of all NHS staff with respect to protecting clinical records from damage, destruction and inappropriate disclosure.

Setting and Achieving an Acceptable NHS standard for information Security Management

Information security is a fundamental component of the overall information governance framework. To support this Code of Practice and in order to assist NHS organisations manage their information securely, an information security management framework will be developed, containing a roadmap, standards, guidelines, tools, methods and other template materials that may be reused in a range of settings. This framework shall be published and maintained independently of this Code of Practice and will be periodically extended to reflect updates to technical, operational and procedural best information security practices.

The roadmap, will identify an outline information security management strategy and outline plan to support both local business objectives and the NHS Connecting for Health agenda. The content of the roadmap will be reviewed and updated at regular intervals and will be published electronically.

Information security management standards ensure the relevant consideration of information security management needs within organisations of all types and sizes. However, it is also important to recognise that such standards, including ISO/IEC 17799:2005, may only identify best practice security management principles and that these principles may be distilled, assessed and applied differently according to each organisation's local business needs and capabilities.

There are several potential sources of information security standards that would be useful to NHS organisations. These include:

- the British Standards Institute's BS7799, now known internationally as ISO/IEC 17799:2005 and its counterpart ISO/IEC 27001:2005 (available to NHS organisations at: www.igt.connectingforhealth.nhs.uk
- the Information Security Forum's *Standard of Good Practice for Information Security Management* (www.isfsecuritystandard.com/index_ie.htm);

- the IT Infrastructure Library's *Security Management* (ISBN 0-11-330014-X);
- the Communications–Electronics Security Group (CESG) information assurance bookstore for the UK public sector.

The above list of information security standards sources is not exclusive, but represents standards known to be in use by NHS organisations within their security management programmes.

To further assist NHS organisations, licensing arrangements have been established with the British Standards Institute (BSI) that allow NHS organisations to download reference copies of the ISO17799 and ISO27001 standards from the Information Governance website for their local use (see https://www.igt.connectingforhealth.nhs.uk for details).

Information security management standards are normally divided into subject areas. For illustrative purposes, ISO17799 and ISO27001 are currently organised into 11 sections, each covering a different topic. These 11 sections are:

- Security policy
- Organising information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and management
- Information security incident management
- Business continuity management
- Compliance.

Whilst the content list of this and other information security standards may initially appear daunting, the key principle is that appropriate controls should be selected, implemented and managed to mitigate the actual risks an organisation faces and that controls should not be implemented simply because they are referred to within the standard.

Many NHS organisations will already have effective security management arrangements in place dealing with these aspects. However, to further assist NHS organisations of all types with their implementation and management of information security, a range of adaptable checklists, templates and supporting materials shall be developed and maintained.

Other Useful Resources

Resource: CESG – The UK Technical Authority for Information Assurance

Location: http://www.cesg.gov.uk

Description: CESG are the UK Government's National Technical Authority for Information Assurance, responsible for enabling secure and trusted knowledge sharing to help organisations achieve their business aims.

Resource: CESG – Directory of InfoSec Assured Products

Location: http://www.cesg.gov.uk/site/publications/media/directory.pdf

Description: This document provides details of information security products tested and assured by CESG.

Resource: CSIA CCT Products Page

Location: http://www.cabinetoffice.gov.uk/csia/claims_tested_mark/awards/

Description: The weblink points to the Cabinet Office-sponsored scheme for the evaluation of commercial products that claim security functionality or value. It is Cabinet Office policy that UK public sector bodies should adopt the scheme where possible. The evaluated product/service listing is expected to expand over time to provide an aid to the selection of information security products to be procured.

Resource: UK Resilience – Civil Contingencies Act

Location: http://www.ukresilience.info/ccact/index.shtm

Description: UK Resilience is a Cabinet Office website. This provides details of the UK Civil Contingencies Act 2004, including a "short guide".

Resource: Get Safe On-line

Location: www.getsafeonline.org

Description: This website points to the initiative supported by UK Government and others, including Microsoft and Ebay, to provide advice and guidance on the safe use of home and small business computers. It includes checklists to test your knowledge of computing risks and issues.

Resource: IT Safe web page

Location: www.itsafe.gov.uk

Description: This is the website for the UK IT Safe initiative. It provides easy to understand news and advice for individuals and small businesses on IT security issues. Users may register with the site for free email updates and new security warnings as they become available.

Resource: NHS Counter Fraud & Security Management Service Division – Forensic Computing Unit

Location: http://www.cfsms.nhs.uk/directorates/fcu.html and http://www.forensic-computing.nhs.uk

Description: The FCU provides a comprehensive and professional service for the benefit of NHS organisations, with qualified forensic computing staff from backgrounds including fraud investigation, statistical analysis and criminal investigation.

Resource: Centre for the Protection of National Infrastructure – Information Security Advisories

Location: http://www.cpni.gov.uk/Products/advisories.aspx

Description: The Centre for the Protection of the National Infrastructure site contains the latest published alerts for consideration and protective action. This information is of particular interest to NHS Trust information security managers and IT support staff with responsibility for the maintenance of system security functionality.

Resource: NHS Connecting for Health – Good Practice Guidelines

Location: http://www.connectingforhealth.nhs.uk/igsecurity/gpg

Description: The Good Practice Guidelines are a series of informative guidance documents providing best practice advice in all areas of Information Governance. This guidance forms part of the NHS Information Security Management framework.

Resource: Information Governance Toolkit – Knowledge Base

Location: www.igt.connectingforhealth.nhs.uk

Description: The knowledge base within the Information Governance Toolkit provides a wide range of exemplar materials, tools and techniques etc to aid NHS and other organisations in improving all elements of their information governance, including information security management.

Resource: Information Commissioner's website

Location: www.ico.gov.uk

Description: The website of the Information Commissioner's Office.

Useful Contacts

Name/title	Organisation	Contact details
	NHS Information Security Policy Mailbox	E: NHSInformationSecurity@dh.gsi.gov.uk
Alistair Donaldson NHS Information Security Policy Manager	Department of Health NHS Connecting for Health	E: alistair.donaldson@dh.gsi.gov.uk E: alistair.donaldson@nhs.net T: 0113 397 4493
Adam Goodwin Deputy NHS Information Security Policy Manager	Department of Health NHS Connecting for Health	E: adam.goodwin@dh.gsi.gov.uk E: adam.goodwin@nhs.net T: 0113 397 4495
Marie Greenfield Information Governance Policy Manager	NHS Connecting for Health	E: marie.greenfield@nhs.net T: 0113 397 4408
Mike Grieveson Head of the NHS Forensic Computing Unit	NHS Counter Fraud & Security Management Service	E: forensics@cfsms.nhs.uk T: 020 7895 4658

DH Department of Health

280361 1p 2.5k Apr 07 (CWP)
Produced by COI for the Department of Health

If you require further copies of this title quote
280361/Information Security Management: NHS Code of Practice
and contact:

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

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

280361/Information Security Management: NHS Code of Practice
may also be made available on request in Braille, on audio, on disk and in large print.

www.dh.gov.uk/publications