Information Security Policy

Author	Aleksandra Foy, Office Manager
Responsible Director	Medical Director
Ratified By	Quality and Safety Committee
Ratified Date	June 2014
Review Date	December 2015
Version	1.1

Related Policies & Guidelines:

- Information Governance Policy
- Information Risk Policy

Contents

Amendment History

Version	Status	Date	Reason for Change	Authorised
1.1		December 2014	Review and formatting	Q&SC

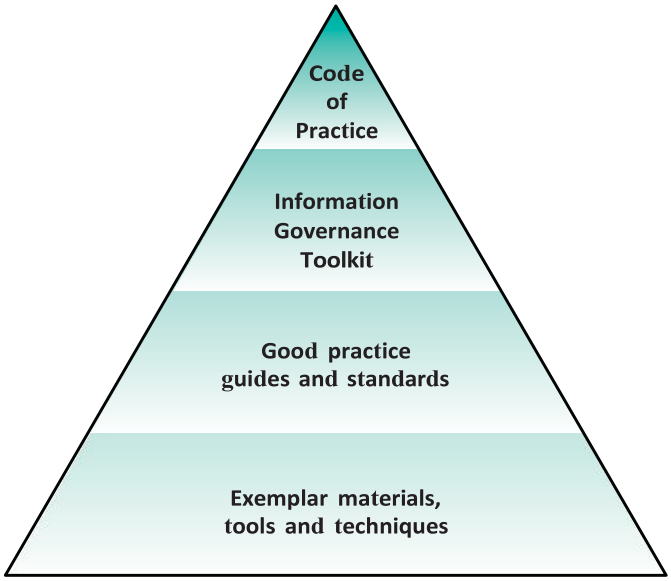
1. NHS Security Code

The Information Security Policy is based on the NHS Code of Practice: Information Security Management.

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.

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.

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.



The NHS Information Security Management Framework

2. Scope

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).

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;
- all Central London Healthcare CIC staff

3. Principles

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 performance, play a key role in ensuring that effective Information Governance systems are in place.

The CLH CIC will be supported in delivering improved information security through the NHS Information Governance Toolkit (IGT). To assist implementation of the this policy an information security management roadmap should be developed.

3.1 General Context

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).

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.

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.

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).

Further information in relation to:

- Monitoring Information Security Management Performance
- Legal and Professional Obligations
- NHS Connecting for Health (NHS CFH)
- Social Care Information

Can be found in NHS Code of Practice: Information Security Management.

3.2 Information Security Policy

The purpose of the 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.

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.

It is the policy of the Central London Healthcare 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;
- organisation-wide business continuity plans is created and implemented for all 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;
- CLH CIC 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.

A comprehensive NHS information security management framework is in place to support this policy. This framework takes the form of this Information Security Policy 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.

4. NHS Information Security Management

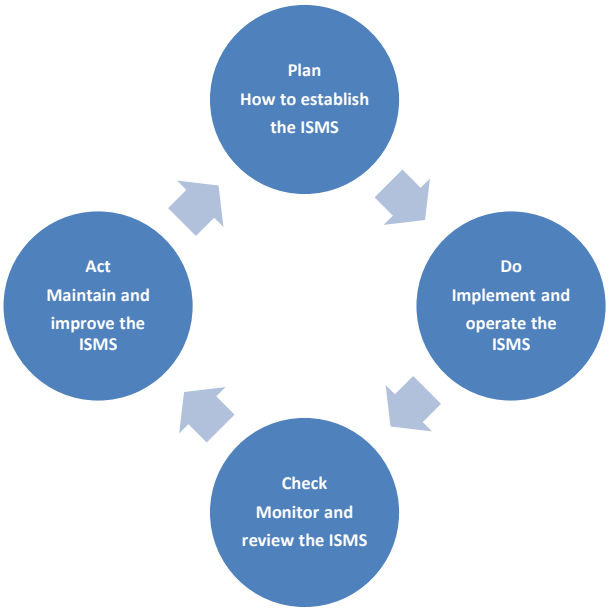
Information Security Policy, supported by Information Security Management: NHS Code of Practice provides the basis for reliable and effective information security management by CLH CIC. It shall be supplemented through a consistent and dynamic range of further guidance, methods, checklists and tools to be developed and that will be applicable to specific information security topics or practices.

4.1 Information Security Management System (ISMS)

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.

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.

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.



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

4.1.1 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.

4.1.2 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.

4.1.3 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.

4.1.4 ACT – Maintaining the ISMS

- Review and update the ISMS as required.

4.2 CLH Organisational Responsibility

Responsibility for information security management is allocated to the Head of Systems (Information Security Lead). It is the Head of Systems' responsibility to ensure 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 is established, implemented, monitored and audited. Those

individuals involved in this aspect of information governance should have clearly defined responsibilities and objectives, and access to adequate resources to achieve them.

Responsibility for information security resides, ultimately, with an organisation's Executive Manager and the Board of Directors. This responsibility is discharged through the Head of Systems to lead information security management within the organisation.

It is essential that the Head of Systems should work in close association with the Service Delivery Managers and Corporate Service Managers responsible for freedom of information, data protection, patient confidentiality and other information governance work areas.

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.

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. As CLH is a small organization it will expect considerable support and advice to be provided by the Central London CCG.

It is the responsibility of team mangers 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.

4.3 Individual Responsibility

All individuals 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.

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 their direct line manager.

4.4 Information Risk Assessment

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.

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.

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.

Appendix 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.

Appendix B – Resources to Support Improvement

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.