NHS
England

Information Security Policy

Information Security Policy

Version number: v2.0

First published:

Updated: (only if this is applicable)

Prepared by: Corporate Information Governance

Classification: OFFICIAL

This information can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request. Please contact england.ig-corporate@nhs.net

Choose an item.

NHS England INFORMATION READER BOX

Directorate		
Medical	Operations and Information	Specialised Commissioning
Nursing	**Trans. & Corp. Ops.**	Strategy & Innovation
Finance		

Publications Gateway Reference:	**08542**
Document Purpose	Policy
Document Name	Information Security Policy
Author	Corporate Information Governance
Publication Date	December 2018
Target Audience	All NHS England Employees
Additional Circulation List	
Description	Policy and high level procedures for Information Security
Cross Reference	
Superseded Docs (if applicable)	Information Security Policy v 3.0
Action Required	To note
Timing / Deadlines (if applicable)	**N/A**
Contact Details for further information	Corporate Information Governance NHS England Quarry House Quarry Hill LS27UE England.ig-corporate@nhs.net

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Contents

1 Introduction

1.1 Background

NHS England is a public body, with information processing as a fundamental part of its purpose. It is important, therefore, that the organisation has a clear and relevant Information Security Policy. This is essential to our compliance with data protection and other legislation and to ensuring that confidentiality is respected.

The purpose of NHS England's Information Security policy is to protect, to a consistently high standard, all information assets. The policy covers security which can be applied through technology but perhaps more crucially it encompasses the behaviour of the people who manage information in the line of NHS England business.

Information security is about peoples' behaviour in relation to the information they are responsible for, facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way.
- Assurance that NHS England is providing a secure and trusted environment for the management of information used in delivering its business.
- Clarity over the personal responsibilities around information security expected of staff when working on NHS England business.
- A strengthened position in the event of any legal action that may be taken against NHS England (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in information security.
- Assurance that information is accessible only to those authorised to have access.

Assurance that risks are identified and appropriate controls are implemented and documented.

1.2 Aim

The aim of NHS England's Information Security Policy is to preserve:

Confidentiality	Access to Data shall be confined to those with appropriate authority.
Integrity	Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
Availability	Information shall be available and delivered to the right person, at the time when it is needed.

1.3 Objectives

The objectives of this policy are to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by NHS England by:

- Ensuring that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other Information Governance policies.
- Working with other Arm's Length Bodies (ALBs) who share a common Open Service supply partner, to develop collaborative approaches, systems and processes relating to information security.
- Describing the principles of security and explaining how they are implemented in the organisation. Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

2 Scope

Staff of the following NHS England areas are within the scope of this document:

- Staff working in or on behalf of NHS England (this includes contractors, temporary staff, embedded staff, secondees and all permanent employees);
- NHS England's Commissioning Support Units

3 Roles and Responsibilities

The information within scope includes:

3.1 Chief Executive

Responsibility for information security resides ultimately with the Chief Executive. This responsibility is discharged through the designated roles of Senior Information Risk Owner (SIRO) and Head of Corporate ICT Technology & and Security as required by the Information Governance Data Security and Protection (DSP) Toolkit.

3.2 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is responsible for information risk within NHS England and advises the Board on the effectiveness of information risk management across the Organisation.

Deputy SIROs have also been appointed in Region Teams to support the SIRO for NHS England.

Hosted bodies, including CSUs will have their own SIRO.

3.3 Data Protection Officer (DPO)

As a public authority NHS England is required to appoint a Data Protection Officer by the General Data Protection Regulation (GDPR). The Information Governance Policy establishes this role. The DPO is responsible for providing advice, monitoring compliance, and is the first point of contact in the organisation for data protection matters. The DPO reports to the SIRO and directly to the Board in relation to data protection matters.

CSUs have appointed Deputy DPOs that report directly to the NHS England DPO.

3.4 Senior Managers

Senior Managers are responsible for the security of their physical environments where information is processed or stored. Furthermore, they are responsible for:

- Ensuring that all staff, permanent, temporary and contractor, are aware of the information security policies, procedures and user obligations applicable to their area of work.
- Ensuring that all staff, permanent, temporary and contractor, are aware of their personal responsibilities for information security.
- Determining the level of access to be granted to specific individuals
- Ensuring staff have appropriate training for the systems they are using.
- Ensuring staff know how to access advice on information security matters

3.5 Head of Corporate Information Governance (IG)

The Head of Corporate Information Governance will be responsible for maintaining appropriate policies and guidance for staff around the use and processing of personal data of information contained within NHS England's information assets in line with data protection and data security legislation and regulations.

3.6 Head of Corporate ICT Technology and IT Cyber Security

The role of the Head of Corporate Information Governance supported by the Head of Corporate ICT Technology and IT Cyber Security.

The Head of Corporate ICT Technology and IT Cyber Security is responsible for developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure NHS England's systems and infrastructure remain compliant with the Data Protection Act 2018.

The Head of Corporate ICT Technology and Cyber Security is responsible for ensuring that all NHS England electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.

3.7 Information Asset Owners

All Information Asset Owners are responsible for ensuring that third party data processors have appropriate ISO and/ or Cyber Essentials accreditation where appropriate for assets stored electronically with third parties. Information Asset Owners are also responsible for ensuring appropriate data protection assurance from all third party suppliers processing NHS England data.

3.8 All Staff

All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action. In particular all staff should undertake their mandatory annual Data Security Awareness training and understand:

- What information they are using, how it should be protectively handled, stored and transferred.
- What procedures, standards and protocols exist for the sharing of information with others.
- How to report a suspected beach of information security within the organisation.
- Their responsibility for raising any information security concerns with the Head of Corporate ICT Technology & and Security.

Contracts with external contractors that allow access to the organisation’s information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

4 Policy Framework

4.1 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause.

Information security expectations of staff shall be included within appropriate job definitions and descriptions.

4.2 Security Control Assets

NHS England Corporate ICT will establish an ICT asset management process and associated system; this will involve support and collaboration from the OpenService vendor where applicable.

All ICT assets, (hardware, software, application or data) shall have a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset.

4.3 Access Controls

Access to information shall be restricted to users who have an authorised business need to access the information and as approved by the relevant IAO.

4.4 Computer Access Controls

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a license from the supplier.

4.5 Application Access Controls

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a license from the supplier.

4.6 Equipment Security

In order to minimise loss of, or damage to, all assets, the Corporate ICT Team shall ensure that all electronic equipment and assets shall be; identified, registered and physically protected from threats and environmental hazards.

4.7 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures. This will also require agreed systems and processes with third party vendors working for and on behalf of NHS England.

4.8 Information Risk Assessment

All information assets will be identified and assigned an Information Asset Owner (IAO). IAO's shall ensure that information risk assessments are performed at least annually, following guidance from the Senior Information Risk Owner (SIRO). IAO's shall submit the risk assessment results and associated mitigation plans to the SIRO for review. Please see the Information Risk Procedures for further information.

4.9 Information Security Events and Weaknesses

All NHS England information security events, near misses, and suspected weaknesses are to be reported to the Head of Corporate ICT Technology & and Security or designated deputy and where appropriate reported as an Adverse

Incident. All adverse incidents shall be reported to the NHS England DPO. The Information Security Incident Reporting procedures must be complied with.

4.10 Classification of Sensitive Information

NHS England shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the Data Security and Protection (DSP) Toolkit to secure their information assets. Further details of the classifications controls can be found in the Records Management Policy.

4.11 Protection from Malicious Software

The organisation and its Corporate ICT service providers shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation’s property without permission from the Corporate ICT Senior Manager or Head of Corporate ICT Technology & and Security. Users breaching this requirement may be subject to disciplinary action.

4.12 Removable Media

Corporate IT systems automatically encrypt removable media. Removable media that contain software require the approval of the Corporate ICT Senior Manager or Head of Corporate ICT Technology & and Security before they may be used on NHS England systems. Users breaching this requirement may be subject to disciplinary action.

4.13 Monitoring System Access and Use

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. NHS England will put in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees’ electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures

- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act and any other applicable law.

4.14 Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks include a System Level Security Policy (SLSP) and are approved by the Head of Corporate ICT Technology & and Security and/or Corporate IT Senior Manager before they commence operation.

4.15 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Corporate IT Senior Manager and the Head of Corporate ICT Technology & and Security.

4.16 Business Continuity and Disaster Recovery Plans

The organisation will implement a business continuity management system (BCMS) that will be aligned to the international standard of best practice (ISO 22301:2012 – Societal security – Business continuity management systems - Requirements).

Business Impact Analysis will be undertaken in all areas of the organisation. Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

The SIRO has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

4.17 Training & Awareness

Data Security and Protection training is mandatory and all staff are required to complete annual on-line Data Security Awareness training.

All NHS England staff are required to read the Information Governance user handbook and accept the declaration. This does not apply to CSUs however a copy of this is available upon request.

4.18 IG requirements for New Processes, Services, Information Systems and Assets

The IG requirements for New Processes, Services, Information Systems and Assets procedure must be complied with when:

- A new process is to be established that involves processing of personal data (data relating to individuals);

- Changes are to be made to an existing process that involves the processing of personal data;
- Procuring a new information system which processes personal data, or the licensing of a third-party system that hosts and or processes personal data.
- Introducing any new technology that uses or processes personal data in any way

5 Distribution and Implementation

5.1 Distribution Plan

This document will be made available to all Staff via the NHS England internet site.

A global notice will be sent to all Staff notifying them of the release of this document.

A link to this document will be provided from the Policy Directorate intranet site.

5.2 Training Plan

A training needs analysis will be undertaken with Staff affected by this document.

Based on the findings of that analysis appropriate training will be provided to Staff as necessary.

Guidance will be provided on the Policy Directorate intranet site.

6 Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Information Governance Team, together with independent reviews by both Internal and External Audit on a periodic basis.

The Head of Corporate Information Governance is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.

7 Equality Impact Assessment

This document forms part of NHS England's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

As part of its development this document and its impact on equality has been analysed and no detriment identified.

8 Associated Documentation

The following documents will provide additional information:

REF NO	DOC REFERENCE NUMBER	TITLE
		Freedom of Information Policy
		Information Governance Policy
		Confidentiality Policy
		Document and Records Management Policy
		Data Protection Policy
		Information Sharing Policy
		Information Governance User Handbook

9 References – legislation

- The Data Protection Act (2018)
- The General Data Protection Regulation
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Health & Social Care Act (2012)

Version Number	Date	Author Title	Status	Comment/Reason for Issue/Approving Body
1.0	12/04//2013	Information Governance Senior Manager	Approved	New policy
2.0	01/06/2014	Head of Corporate Information Governance	Approved	Yearly review
3.0	14/06/2016	Head of Corporate Information Governance	Approved	Yearly review
4.0	August 2018	Data Protection Officer	Draft	Updated to comply with new data protection legislation

NHS England 2018

First published April 2013