



Cancer Screening Programmes

NHS Cancer Screening Programmes

Information Security Policy

VERSION 3

JULY 2009

NHS Cancer Screening Programmes

Information Security Policy

1 Introduction and Scope

This document has been adapted from the NHSIA national template. Units and departments should work with their local IT advisors for the Trust or health organisation in order to ensure its effective adoption. It defines the Information Security Policy for the NHS Cancer Screening Programmes in England and covers all information (in all its forms), information systems, environment and relevant people who support the programme. This document:

- sets out the Programmes' policy for the security of information (especially with regard to Confidentiality, Integrity and Availability); and
- establishes the responsibilities for information security.

The NHS Cancer Screening Programmes place a very high importance on the security of information maintained and processed on behalf of the NHS and patients. It is the responsibility of all staff involved in the programmes to comply with this policy and other relevant legislation, together with any supporting policies and procedures local to the host Trust or Authority. **Failure to comply may result in disciplinary procedures being instigated by the host employer.**

2 Policy Aims

The policy aims to ensure that:

1. Computer systems are properly assessed for security
2. Confidentiality, integrity and availability are maintained
3. Staff are aware of their roles, responsibilities and accountability
4. Procedures to detect and resolve security breaches are in place

Staff working in each part of the NHS Cancer Screening Programmes will be made aware of the statutory, regulatory and guidance framework and local related policies as agreed by the host employer. Local policies must take into account the following documents:

- Baseline NHS Security Standards as listed in NHS IM&T Standards Handbook
- BS7799 to the extent of the Scope described in the Information Security Management System (ISMS) documentation
- NHS Net Acceptable Use Policy
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Access to Health Records Act 1990
- The EC Directive on Legal Protection of Databases 1996 (Directive 96/9/EC of the European Parliament and the Council of 11 March 1996 on the legal protection of databases)
- The Caldicott Report 1997 (The Caldicott Committee: Report on the Review of Patient-Identifiable Information - December 1997)
- Data Protection Act 1998
- Human Rights Act (1998)
- Electronics Communications Act 2000
- Freedom of Information Act 2000
- Health and Social Care Act 2001
- Mental Capacity Act 2005

3 Policy Objectives

Confidentiality, Integrity and Availability

The purpose of the security policy is to preserve:

Confidentiality: Data access is confined to those with specific authority to view the data.

Integrity: All information systems operate correctly according to specification.

Data must not be unexpectedly modified, either accidentally or wilfully.

Availability: Information is available when required.

All NHS Cancer Screening Programmes staff are expected to be familiar with policies and procedures that relate to confidentiality and data protection and to comply fully with the current legislation.

Physical Security

Only authorised personnel and their official visitors will be permitted access to premises where NHS Cancer Screening Programmes' information is stored. The host employer is responsible for the security of areas housing servers, networking equipment and paper records associated with the programmes.

Protocols should be in place for the use of equipment utilised by the Programmes outside of such premises in order to protect that equipment and the information to which it allows access.

Equipment and Software Procurement and Disposal

All software and equipment will be procured using procedures that ensure that a register of information assets is maintained by the local employer and that breaches of confidentiality or software copyright do not occur. These include POISE and EC regulations together with the disposal of hardware and data.

Risk assessment

Each part of the NHS Cancer Screening Programmes will carry out, in conjunction with host organisations, security risk assessment(s) in relation to all the business process covered by this policy. These risk assessments will cover all information assets, applications and networks that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

System Security Policies

System Security Policies will be produced by host employers for all information systems, applications and networks. These policies will be developed on the basis of the risk

assessment.

Secure Operating Procedures

Working in conjunction with the host employer, the local screening programme must produce detailed relevant Secure Operating Procedures to ensure compliance with the local System Security Policies. All users of the systems must be made aware of the contents and implications of relevant System Security Policies and Secure Operating Procedures. These local detailed procedures will:

- a. require all information systems, applications and networks involved in the programmes to be approved by the host employer before they commence operation
- b. require an effective configuration management system for all relevant information systems, applications and networks
- c. require authorised staff only to have access to those information systems maintaining and processing the Programmes' information
- d. require measures to be in place to detect and protect information systems, applications and networks from viruses and other malicious software
- e. require all connections to external networks and systems have documented and approved System Security Policies. The host employer must approve all connections to external networks and systems before they commence operation
- f. require all operational applications, systems and networks to be monitored for potential security breaches. All real or potential security breaches including suspected incidents and security weaknesses, must be reported and investigated in accordance with NHS incident reporting schemes
- g. require contingency plans and disaster recovery plans to be produced for all critical applications, systems and networks. The plans must be reviewed by the host employer and tested on a regular basis
- h. require that members of staff do not commence employment until adequate checks have been performed into their background and identity

- i. require security awareness training is provided for all staff and updated annually, to ensure that they are aware of their responsibilities for security, and the actions that they need to undertake in order to discharge those responsibilities, including an understanding that irresponsible or improper actions may result in disciplinary action(s) being instigated by the host employer.

4 Security Responsibilities

Overall Responsibilities

Responsibility for implementing this policy within the context of relevant IT systems will lie with the relevant host employer.

Management Responsibilities

Directors of breast screening, the Director for colorectal screening, lead pathologists, lead colposcopists or hospital-based co-ordinators for cervical screening, screening commissioners for the appropriate PCTs for the recall system and acceptance data, Quality Assurance Directors and Director, NHS Cancer Screening Programmes are each, in their own departments, responsible for:

- making arrangements for information security by complying with the overall information security policy for the host organisation
- assigning responsibility for information security

- operating within parameters set by the host organisation's Information Security Manager
- operating within parameters set by the host organisation's Data Protection Officer
- ensuring the security of the Programmes information and associated assets, hardware and software used by staff and, where appropriate, by third parties is consistent with legal and managerial requirements and obligations
- ensure that, where appropriate, staff receive IT security awareness and training
- ensuring that Programmes' staff are aware of their security responsibilities.

General Responsibilities

All staff are responsible for information security and therefore must understand and comply with this policy and the supporting policies available on the NHS or Trust Intranet, etc. It is the duty of each employee who uses or has access to information to be aware of and abide by the procedures and arrangements concerning the secure use and protection of information.

All personnel or agents acting for the organisation have a duty to:

- safeguard hardware, software and information in their care
- prevent the introduction of malicious software on the organisation's IT system
- report any suspected or actual breaches in security.

5 Validity of this Policy

This policy is effective immediately and will be reviewed annually under the authority of the Programmes' National Coordination Team, before PIAG review submission. Associated information security documents will be the subject of a continuing development and review programme.