NHS
North Yorkshire and York

Title:	**USE OF ENCRYPTION TECHNOLOGY POLICY**
Reference No:	NHSNYYIG-013
Owner:	Director of Standards
Author:	Information Governance Team
First Issued On:	August 2010 (version 1.00)
Latest Issue Date:	February 2012 (version 1.001)
Operational Date:	February 2012 (version 1.001)
Review Date:	August 2013 (Version 1.001)
Consultation Process:	JNCC, LNC, JEPF
Policy Sponsor:	Director of Standards
Ratified and Approved by:	Information Governance Steering Group Governance & Quality Committee
Distribution:	All staff
Compliance:	Mandatory for all permanent & temporary employees, contractors, sub-contractors of and those who work jointly with North Yorkshire and York PCT
Equality & Diversity Statement	This policy has been subject to a full equality & diversity impact assessment

CHANGE RECORD			
DATE	AUTHOR	NATURE OF CHANGE	VERSION No
24.02.2010	Info Gov Mngr	First Draft	0.001
18.05.2010	IG Team	Policy amendments	0.001
23.05.2010	A Wood	Policy amendments	0.002
31.08.2010	IG Team	Policy Approved	1.000
14.12.2011	IG Team	Amendments to reflect the new organisational structure	1.001

1. Introduction

The NHS is committed to the delivery of a first class confidential service. This means ensuring that all patient information is processed fairly, lawfully and as transparently as possible so that the public:

- understand the reasons for processing personal information;
- give their consent for the disclosure and use of their personal information;
- gain trust in the way the NHS handles information and;
- understand their rights to access information held about them.

Definition of the Term Sensitive Information as used in this document
NYY PCT must ensure that all sensitive information being processed by the organisation is appropriately secured. The guidance below sets out the requirements for handling such information.
Sensitive information can include (but is not limited to) personal data relating to any individual e.g. patients, members of staff etc, as well as potential sensitive business information such as business and supplier contracts and any information which would be exempt from provision under the Freedom of Information Act 2000.

2. Scope

This policy applies to all employees of the PCT in all locations including the Non-Executive Directors, temporary employees, locums, contracted staff and volunteers and with those who the PCT contracts with to process information on their behalf.

3. Responsibilities

Chief Executive - The Chief Executive has overall responsibility to ensure that the PCT complies with all legal obligations, relevant legislation, standards and guidelines in respect of securing information held and used by the organisation.

Director of Standards - Is the NHS NYY nominated Senior Information Risk Officer (SIRO) and therefore is the designated member of staff who has lead responsibility for information security and risk within the organisation.

Directors, Senior and Line Managers - Are responsible for ensuring that all staff are aware of and understand their obligations and duties in line with this policy.

Information Governance Manager - Will support the SIRO and Information Asset Owners in the implementation of appropriate Information security controls. In addition will assist and advise on information security incidents investigation and report all such incidents to the Information Governance Steering Group.

Information Asset Owners (IAO) - An IAO are senior members of staff who are nominated owners for one of more information assets of the organisation. They must understand the overall business goals of the organisation and how their information assets contribute to or affect these goals. IAOs will document understand and monitor

- What information assets are held and for what purposes
- How information is created amended or added to over time
- Who has access to the information and why

PCT Employees - Employees are responsible for:

- The security of information that they create or use in the performance of their duties.
- Reporting any suspected or known breaches of information security, or identify weaknesses within information systems they may use, to the Information Governance Manager.

4 Purpose

The purpose of the Use of Encryption Technology 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 through compliance with IS027001.

Corporate Data

The Freedom of Information Act 2000 places responsibilities on Public Authorities to provide access to the corporate information it holds by two methods. Firstly by the provision of information through a corporate Publication Scheme, and secondly, subject to exemptions, by providing responses to requests for information. The Act also places responsibilities to have appropriate records management policies and processes in place.

Personal Data

- The Data Protection Act 1998 defines personal data as data which relates to a living individual that can be identified
    - From those data, or
    - From those data and other information which is in the possession of or is likely to come into the possession of the (data controller) NHS North Yorkshire and York (the organisation),
    - And includes any expression of opinion about the individual and any indication of the intentions of the organisation in respect of the individual.

- The following personal data is classed as **sensitive personal data** and stronger safeguards must be in place in relation to it
  - The racial or ethnic origin of the individual
  - Political opinions held
  - religious beliefs or other similar beliefs of a similar nature
  - trade union membership
  - information relating to physical or mental health or condition
  - sexual life
  - commission or alleged commission by the individual of any offence, or
  - any proceeding for any offence committed or alleged to have been committed, and any sentence of any court in such proceedings.

5 The Caldicott Principles

Caldicott Principles -The Caldicott report relates to the use of patient-identifiable information within the NHS and highlighted two key points:

- All NHS organisations must appoint a Caldicott Guardian, and
- details six key principles to be applied when using patient – identifiable information.

Compliance with these principles reduces the risk of breach of confidentiality and breaking the law. These principles detail best practice and should therefore also be adopted when dealing with all personal information and confidential corporate information. The principles are as follows:

1. Justify the purpose(s) of using confidential information

Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

2. Do not use patient-identifiable information unless it is absolutely necessary

Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that information flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary patient-identifiable information that is required

Where use of the patient-identifiable is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

4. Access to patient-identifiable information should be on a strict need-to-know basis

Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

5. Everyone with access to patient-identifiable information should be aware of their responsibilities

Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Understand and comply with the law

Every use of patient-identifiable information must be lawful. Each organisation handling patient information is responsible for ensuring that the organisation complies with the legal requirements. The Caldicott Guardian and Lead and the Information Governance Team can provide guidance.

6 Encryption Technology

To meet NHS requirements **all** removable media and portable devices used to store the organisation's information electronically must be appropriately authorised and encrypted and all electronic transfers, outside of the local secure network, of sensitive information held electronically must be appropriately authorised and encrypted.

To support these requirements the organisation is putting technical controls in place on its network. The controls will operate to prevent the transfer of information from the secure network to unauthorised devices and to prevent unauthorised transfers.

It is required that equivalent controls are in place and documented as part of a written contract between the organisation and any partners, third parties and / or stakeholders who process the organisation's sensitive information.

Any transfer of sensitive information must be tracked. Tracking requirements are detailed in the organisations Record Management Policy.

Is it necessary to hold sensitive information on portable storage devices?

- It is important to understand that the requirement to hold sensitive information on any electronic storage device away from the secure network storage provided centrally should be minimal and temporary and must only be used when there are no secure mechanisms in place to access the information centrally.

- Sensitive information that is stored away from the central network has a greater vulnerability to unauthorised access.
- The process of storing or transferring sensitive information to storage devices away from the secure network storage must only occur where there is an appropriately approved business requirement.
- Processes must be in place to ensure that sensitive information is securely moved and removed from portable storage devices to the secure network storage as soon as possible. This is essential where portable devices are used to capture information and the only instance of the information is held on portable devices
- Sensitive information must not be held on portable media unless the storage devices are appropriately approved and encrypted
- Report any data or device loss or any compromise of controls immediately via the corporate incident reporting system

Where there is an appropriately approved operational requirement to hold sensitive information on encrypted portable storage devices the following safeguards have been put in place to protect sensitive information that is not stored on the secure network storage systems.

It is each individual's responsibility to ensure the security of the portable devise they have installed sensitive information on.

7 Laptops

- **All** Laptops **must** have full disk encryption installed on them. This ensures that the hard disk of the laptop is encrypted and affords protection to the data held on it.
- If you have organisational laptop that **does not** have encryption software installed, you **must** contact the IT Service Desk immediately.
- Do not take any laptop with sensitive information stored on it out of the office until encryption technology has been installed.

8 Removable Storage Media

- **Only** use the approved encrypted Removable Storage Media e.g.USB Data Sticks etc issued by the organisation
- Methods of working must be addressed to ensure that there is not an operational need to hold sensitive information on Removable Storage Media.

- If you have organisational Removable Storage Media that **does not** have encryption software installed, you **must** contact the Service Desk immediately.
- Do not take any organisational Removable Storage Media with sensitive information stored on it out of the office until encryption technology has been installed.
- If you have Removable Storage Media that is not encrypted and or not issued by the organisation any sensitive information must be transferred to the secure network and then securely removed from Removable Storage Media. Please contact the Service Desk immediately if this is the case.

9 Blackberries

- Only use encrypted blackberries which have been approved and issued by the Informatics Department.
- If you have an unencrypted PDA you must stop using it and contact the Service Desk immediately.

10 Other Storage devices

- Encryption technology meeting the required standards and approved by the Informatics Department must be used if data is stored on other storage devices that will be used to transport or hold sensitive information or used as devices to back up data.
- Do not store sensitive information on either CDs or DVDs as these media are easily readable on most computers and the data cannot be easily secured using encryption.
- Do not take storage devices with sensitive information stored on them out of the office unless the approved encryption technology has been utilised.

11 Secure electronic data transfer methods

- The organisation uses encrypted methods of electronic data transfer and only these should be used to transfer sensitive information with appropriate authorisation. The Informatics Department can provide information on approved methodologies. It is not permitted to use unapproved methods of electronic transfer.

12 Email

NHSmail is the only secure email system and directory service for NHS staff in England and Scotland, approved for exchanging sensitive information with NHSmail and GSi users.

Staff can get an NHSmail address for their whole NHS career and it is accessible anywhere.

The following are the approved secure accounts that link to NHSmail.

NHS (*.nhs.net)
GSi (*.gsi.gov.uk)
CJX (*.police.uk or .pnn.police.uk)
GSE (*.gse.gov.uk)
GSX (*.gsx.gov.uk)
GCSX (*.gcsx.gov.uk)
SCN (*scn.gov.uk)
CJSM (*cjsm.net)
MoD (*.mod.uk)

Sensitive information must only be transferred with appropriate authorisations and safeguards, such as approved encrypted email, e.g. NHSmail.

13 Securing Data in Transit

The Information Security Policy details requirements for sending information securely and must be referenced in conjunction with this policy, however as a minimum:

- Do not bulk transfer sensitive information unless it is absolutely necessary and meets the requirements of the Caldicott Principles and that the transfers are appropriately approved and authorised. For the definition of bulk transfer see the Information Minimum Security Measures at http://nww.northyorkshireandyork.nhs.uk/Corporate/InformationGovernance/PoliciesGuidelines.htm

- Once appropriately authorised all transfers sensitive information must be encrypted using approved technology
- Ensure that encrypted sensitive information is trackable throughout its journey
- Ensure that you are notified when it has reached its destination
- Prior to encrypted transfer ensure that there are appropriate documented security measures that comply with ISO27000 series in place within the organisation you are transferring the data to.

14 Technical controls to support the protection of information

Software has been installed onto the organisations network to support the protection of information and to ensure that only authorised equipment is used to store or transfer information. The software will control the use of storage devices connected to the network

- Only authorised encrypted Removable Storage Media will be permitted
- The writing of information to CDs DVDs or other unapproved or unauthorised storage devices will not be allowed
- The transfer of information other than by authorised secure transfer mechanisms will not be allowed

15 Vulnerable Equipment Hard Drives

- The writing of information to the hard disk of any networked desk top computer is not allowed and all data should be stored on the secure network.
- Where appropriate all laptops will synchronise to the appropriate network drives when logged onto the network.

Exceptions

All exceptions to this policy must be approved by the SIRO and / or the Information Governance Steering Group as appropriate, and presented in the form of a documented risk assessment which includes an appropriate supporting business case.

16 Training and Awareness

- Information Governance and security training is required for all staff and is included as part of the induction and statutory and mandatory training.
- Staff will be made aware of this policy via line management.
- This policy will be available to all staff via the PCT Intranet.

17 Equality and Diversity

The PCT recognises the diversity of the local community and those in its employ. Our aim is therefore to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. All policies and procedures are assessed in accordance with the Equality & Diversity Assessment Toolkit, the results for which are monitored centrally.

18 Freedom of Information Act 2000

Any recorded information which is held by, or on behalf of, the PCT may be subject to disclosure under the Freedom of Information Act 2000 and Environmental Information Regulations.

19 Records Management

Records provide evidence and information about the business activities of the PCT and are corporate assets of the PCT. This policy should therefore be retained in line with the NHS Code of Practice on Records Management (Department of Health, 2006). Compliance with this code will ensure that the organisation's records are complete, accurate and provide evidence of and information about the organisation's activities for as long as is required.

20 Review

This policy will be reviewed annually. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation or guidance.

21 Monitoring

- Breaches in Information Security must be reported via the PCT's incident reporting mechanisms and will be subject to investigation and reported to the Information Governance Steering Group
- The Audit Commission regularly conducts studies into information security management.
- The NHS Litigation Authority also assesses risk management arrangements through its NHSLA/CNST standards.

22 Discipline

Breaches of this policy will be investigated and may result in the matter being treated as a disciplinary offence under the PCT's disciplinary procedure.