

Guidelines on use of encryption to protect person identifiable and sensitive information

1. Introduction

David Nicholson, NHS Chief Executive, has directed that there should be no transfers of unencrypted person identifiable data held in electronic format across the NHS. This is the default position to ensure that patient and staff personal data are protected. Any data stored on a PC or other removable device in a non-secure area or on a portable device such as a laptop, PDA or mobile phone should also be encrypted. This is also now a requirement across all public sector organisations set by the Cabinet Secretary.

It is recognised however that this may take some time to achieve in the NHS where patient care is our highest priority. NHS bodies will need to make a local judgement on the balance of risk to patient care against risk to personal data security in determining whether use of unencrypted devices should continue as an interim measure. Where it is felt that continued reliance upon unencrypted data is necessary for the benefit of patients, the outcome of the risk assessment must be reported to the organisation's Board, so that the Board is appropriately accountable for the decision to accept data vulnerability or to curtail working practices in the interests of data security.

2. Data encryption applications

NHS Connecting for Health is already implementing a robust NHS information governance architecture that contains strong in-built encryption functionality for those core services it provides. Security services implemented within this architecture protect the flows of patient information between component parts of connected national and local applications, and automatically encrypt transmission of emailed information communicated through the NHSmail service between NHSmail endpoints. Tools are also provided within applications provided by NHS CFH for encrypting removable media as explained at Annex A.

For those other systems under local NHS organisation control, there is a requirement that the owners of those systems should consider, select and where relevant implement similar security protections that comply with expected NHS Information Governance policy, standards and legal requirements¹. Guidance on potential encryption tools is provided at Annex B.

¹ The NHS Code of Practice on Information Security can be found at http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_074142

NHS Information Governance

NHS organisations should adopt a structured approach to the identification, implementation and management of their local data encryption needs. This will normally comprise five stages:

- Perform risk assessment and identify outline data encryption needs;
- Develop a local data encryption policy;
- Establish local roles and responsibilities;
- Define how data encryption will operate within the local infrastructure and with business partners including business impact analysis;
- Implement and monitor deployed solution effectiveness.

An encryption requirements control form is provided at Annex C to supplement this guidance and will be helpful in locally developing these stages.

3. NHS Information Governance data encryption standards

For those systems under local NHS control, the Electronic Government Interface Framework (E-gif) Technical Standards Catalogue version 6.2 identifies current technical security standards, including those for data encryption that should be applied. This catalogue is available to download at http://www.govtalk.gov.uk/schemasstandards/egif_document.asp?docnum=957

In brief summary, the NHS IG data encryption algorithms currently applicable are:

- **3DES (168bit)**
- **AES 256**
- **Blowfish**

These algorithms should be used with a recommended minimum key length of 256 bits where available. This is the standard we are moving towards and whilst tactical deployments of less robust encryption are acceptable for now this should be kept under review and stronger encryption introduced when practicable.

Where data is to be transferred across the internet or by removable media it is recommended that AES256 encryption is employed. This standard is available when using applications such as PGP or WINZIP version 9. With these products the data can be put into a Self Decrypting Archive (SDA) as the software that created the archive does not need to be installed on the recipients' computer. The pass phrase for the archive must be of an appropriate length and complexity. To ensure the safety of data in transit the pass phrase should be communicated to the recipient separately from the encrypted data so that the intended recipient is the only one able to decrypt the data.

NHS Information Governance

A comprehensive technical good practice guideline overview of Approved Cryptographic Algorithms, including Secure Sockets Layer (SSL) and Transport Layer Security (TLS) has been produced by NHS Connecting for Health and is available for download at

<http://nww.connectingforhealth.nhs.uk/infrasec/gpg/acs.pdf>

NHS Connecting for Health has completed the national procurement of an encryption solution for removable media and full disk encryption on behalf of the NHS. For all the latest information relating to the NHS encryption tool initiative please see the encryption tool website, at:

<http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/encryptiontool>

Any further queries can be directed to cfh.encryptedtool@nhs.net

Digital Information Policy
Department of Health
31 January 2008

CfH provided encryption technologies

Throughout the NHS technologies are available to organisations which may satisfy some requirements for the encryption of sensitive data. It should be noted though, that encryption products do have some inherent risks and these should be fully understood before implementing any solution. Understanding these risks is probably best achieved by conducting an appropriate risk assessment. There is also the need to determine that the specified business requirements will be met via the encryption product.

Microsoft Operating Systems

Microsoft Windows operating systems incorporate technologies which enable administrators to allow sections of the file system to be used such that documents (files) stored in those areas are encrypted. The implementation of encryption within the Microsoft Operating System suite varies between versions of the OS, a brief overview is shown below and further information can be found in the forthcoming Advice and Guidance document previously mentioned.

Encrypting File System (EFS)

Microsoft offers a technology known as Encrypting File System (EFS) and the capabilities of this technology have improved in later versions of the Operating System. It should be noted that whilst the DESX algorithm is not recommended as meeting required encryption standards, it may be suitable in some cases where a short term solution is required.

Microsoft Version	Default Algorithm	Notes
Windows 2000	DESX	Deployable only in standalone configuration
Windows XP RTM	DESX	Policy based domain integration
Windows XP SP1 and above	AES	
Windows Vista / Server 2008	AES	Bitlocker features available

The use of encryption in prior versions of Microsoft Operating Systems is reliant upon third party software which may not meet current encryption standards and may not include continuing support.

It should be noted that EFS is enabled 'by default' in all versions of Microsoft Windows from Windows 2000 onwards unless its usage has been disabled via Group Policy or at installation. This may in itself represent a problem in that users within organisations could be using EFS presently unbeknownst to

administrators and without proper control or management of the encryption keys.

Prior to organisations using EFS, there are a number of considerations which need to take place including:

- What systems EFS should be used upon (often, this is mobile devices, but could be desktop computers assessed as vulnerable to theft)
- Which files/directories users should be able to use EFS with²
- Who the Data Recovery Agents (DRA's) will be (i.e. those users who can recover encrypted data where the certificate used for encryption has been lost, deleted, revoked or corrupted.)
- Whether certificates for use with EFS will be issued via a centralised (to the host organisation) certificate issuing authority (preferred) or whether self-signed certificates will be used
- How certificates will be managed to enable EFS to be used in such a way that either the keys or the encrypted data can be retrieved if they are lost or corrupted
- Providing appropriate advice and guidance to users on how to use EFS
- Understand that the initial encryption of large amounts of data when first enabling EFS on an existing operating system installation may take some time.

These considerations and others are vital to ensure that EFS use is managed and controlled in a way that meets the organisations and any regulatory/legal requirements.

BitLocker Drive Encryption

The 'Enterprise' (covered by the NHS Microsoft Enterprise Agreement) and 'Ultimate' (the premier consumer edition) versions of Windows Vista contain a technology known as 'BitLocker'. Unlike EFS which only allows files and directories to be encrypted, BitLocker provides full volume encryption akin to the type of full disk encryption previously only provided by 3rd party products. The Enterprise edition of Windows Vista is available to all NHS organisations who buy a copy of Microsoft Windows Vista Business with any new hardware (or who buy a boxed version of Microsoft Windows Vista Business through a reseller in order to upgrade existing hardware). BitLocker is not available on Microsoft Windows XP or Windows Vista Business.

² The CUI document, 'Microsoft Infrastructure Security Guidance' provides a sample script which could be rolled out to appropriate systems to allow certain areas of the file system to use EFS as well as additional guidance on the use of EFS. This document is available from <http://nww.cui.nhs.uk/> (N3 link and registration required.)

As with EFS, it is necessary to ensure that appropriate considerations are taken into account before using BitLocker and that it will meet the organisations business requirements. Some such considerations are:

- BitLocker requires a Trusted Platform Module (TPM) v1.2 chip available on the system it is to be enabled on³
- Determine which systems within the organisation will use BitLocker (generally, this would probably be laptops though it could be used on any system running Vista Enterprise which holds sensitive data which needs to be protected 'at rest'.)
- The hard disk of the computer running Windows Vista Enterprise must be appropriately partitioned
- A method of managing the recovery key used by BitLocker in the event of loss or damage of the startup key needs to be put in place. Where will such keys be securely stored and how for example.
- Determine whether BitLocker will be enabled on systems at first use or whether it is necessary to enable it on systems that have already been deployed.
- Understand that there may be a small performance impact on systems with Bitlocker enabled (although this is unlikely to be noticeable on new hardware).
- Understand that initial encryption of the disk can take some time depending on system performance and size of volume⁴

As with EFS, there are many important considerations to take into account prior to enabling BitLocker on applicable systems, not least that its use meets business as well as regulatory/legal requirements.

³ It is actually possible to get BitLocker working on systems without a TPM chip via Group Policy. See <http://technet2.microsoft.com/WindowsVista/en/library/c61f2a12-8ae6-4957-b031-97b4d762cf311033.mspx?mfr=true> (Section 3). Note that using this method may not provide enough protection to the startup key for BitLocker unless the keys are properly protected via other means.

⁴ Microsoft suggests that 1G gigabyte per minute is usual. See the BitLocker FAQ: <http://technet2.microsoft.com/WindowsVista/en/library/58358421-a7f5-4c97-ab41-2bcc61a58a701033.mspx?mfr=true>.

Interim Encryption Solutions for Data Security

Context

The use of encryption to secure sensitive data which is stored and transmitted throughout the NHS is a crucial requirement to ensure that the confidentiality of data is maintained. This guidance provides information relating to a number of products which may be used as interim measures to protect data prior to the procurement of solutions which may provide greater management capabilities and control of data encryption.

Guidance

The following guidance provides detailed information relating to products which can be obtained readily on the internet. These products include freeware and open source alternatives to commercially available products; by their nature they may not have technical support available and should be used with appropriate care.

Please note that listing of these or any product here does not constitute a recommendation or endorsement of any specific vendor or encryption product or a recommendation to download, buy or install any specific product by NHS Connecting for Health.

TrueCrypt (<http://www.truecrypt.org/>)

TrueCrypt provides encrypted container files which can be mounted as logical drives within the operating system. A variety of encryption algorithms are available within the product and creation of encrypted volumes is extremely easy. TrueCrypt can be used in two ways to provide security of data at rest on a computer and also to protect mobile data on removable media.

TrueCrypt does not provide any centralised management features therefore the backup of keys and the encrypt volumes themselves must be managed by the user or suitable support function. It is critical that the backups are made of the TrueCrypt volumes themselves, the header files of the volumes, any key files used and the passphrase to access the volume for recovery purposes.

Guidance is provided below to enable users to make a suitable backup of the header of TrueCrypt volumes for recovery purposes and also how to configure TrueCrypt for removable media.

Backing up the TrueCrypt volume header

When creating a TrueCrypt volume for the first time, a passphrase should be chosen which can be stored with the volume header which will not be used for regular mounting of the volume. Once the volume has been created, select the volume file and utilise the *Backup Header* tool within the Tools menu. This will create a backup file of the current volume header which should be burnt to CD or stored securely along with the passphrase which was used to create the volume.

Once the header has been backed up, the volume passphrase may be changed to a value which meets the requirements of the local password policy. The volume may now be mounted by supplying the passphrase and selecting the drive letter to be associated with the volume. Once mounted, the volume appears simply as a drive letter and files may be dragged and dropped as required. When no longer required, the volume can be dismounted and all the files which had been saved on the mounted drive will be rendered inaccessible without the passphrase (and key files if used).

Using TrueCrypt in Traveller Mode

TrueCrypt offers a feature which will enable users to secure data on rewritable removable media such as USB memory sticks and memory cards. This mode copies only the required files to the USB stick and creates an encrypted volume which can be mounted when the USB stick is inserted into a computer. Note however, Administrator privileges are required to run a USB stick in Traveller mode for the first time on a machine due to the need to install a device driver.

To create a Traveller Disk, select 'Traveller Disk Setup' from the Tools menu within the TrueCrypt main window. Select the appropriate USB device for the root files and determine what actions to take when the device is inserted. For devices which will be used frequently, it is recommended that the Auto-Mount option is selected and that the password is NOT cached in memory. Once the setup has created the relevant files the user will have to create a TrueCrypt volume using the new volume utility at the location which was specified in the Traveller setup.

As with all TrueCrypt volumes, the guidance above on the backup of a suitable file header and passphrase is highly recommended to ensure access to data if the working passphrase is lost or forgotten.

Gnu Privacy Guard (<http://www.gnupg.org/index.en.html>)

Gnu Privacy Guard (GPG) is the open source alternative to the commercially available PGP which provides comprehensive integration and centralised management. GPG provides the core encryption capabilities required to encrypt and sign files or sign emails. The algorithms which are available within this software meet or exceed the standards which have been provided by the NHS CFH IST Approved Cryptographic Algorithms Good Practice Guideline⁵.

GPG does not provide any central management functions and should be considered as a standalone product which will require additional local support to ensure that critical files are backed up securely.

Cryptainer LE (<http://www.cypherix.co.uk/cryptainerle/index.htm>)

Cryptainer LE is a free version of the commercial Cryptainer software which offers similar capabilities to TrueCrypt although the free version has a limit of

⁵ <http://nww.connectingforhealth.nhs.uk/infrasec/gpg/acs.pdf>

25MB for secure containers. This product also offers encryption of individual files using the Blowfish algorithm and when utilising this feature, strong passphrases should be used to secure the data against a brute force attack.

Securing a file for delivery by email or on removable media

Cryptainer LE provides the ability to encrypt individual files; this can be accessed by clicking on the Secure Email link on the main Cryptainer LE window. Once the required file has been selected, a passphrase should be entered to secure the file against brute force attacks. It is recommended that an 'Encrypted Self-Extractor' file is created which will not require any software to be installed on the destination machine; this may cause problems with some email systems which do not allow executable files to be transmitted and may be best suited to transfer on removable media.

There is no 'backdoor' access to the files which are created by Cryptainer LE and therefore the security and availability of the passphrase are crucial. If an encrypted file may be required for an extended period of time, the passphrase should be noted and stored securely in a physically secure area such as a safe which has restricted access.

AxCrypt (<http://www.axantum.com/AxCrypt/Features.html>)

AxCrypt is a software package which allows users to encrypt files through the standard Windows explorer right-click menus and provides AES-128 encryption. Once installed (requires Administrator rights) the user can simply right click on a file to encrypt it by providing a passphrase. It should be noted that the recipient of the file will require either the full version of AxCrypt or the AxDecrypt utility to decrypt the file with the relevant passphrase.

General Guidance on the use of encryption products

The use of encryption products can provide an organisation with a measurable increase in overall security although there are a number of areas which must be taken into consideration with products similar to the ones mentioned within this guidance. Non-commercial (and some commercial) products may not provide the relevant management functionality which will be required by larger organisations to support large user bases. The types of products which are available to individuals may only meet interim needs whilst other products are procured.

Requirements for the local use of data encryption products (page 1 of 3)

The following record will assist NHS organisations to identify local requirements for data encryption and how they will address them. The form may be used in conjunction with centrally procured NHS encryption tools, or where this is not possible for those encryption tools procured locally. A record should be provided for each use of encryption in the organisation.

Name of individual completing questionnaire:		Business area:
Title:	Date:	Signature:

Name of cryptographic product:	Name of business system:
Provide an overview of what the product is used for and the scale of usage:	
Rationale for use	
What are the vulnerabilities being addressed?	
Provide details of any formal risk analysis carried out and of the business case made:	
Individual responsible for authorising usage:	
Is this a tactical or a strategic solution?	
Provide details of any known plans for changes or extent of usage for this product:	
Operational management arrangements	
Who is responsible for operational management?	
Provide details/references for any documented operating standards and procedures:	

NHS Information Governance

Provide details of the extent of usage, for example, number of licenses for software products or number of units for hardware products:

For physical devices provide details of their physical location:

Details of physical protection mechanisms to prevent tampering/misuse:

Technical aspects

Product name and version
Supplier/source
Algorithms used
Key lengths used

Key management arrangements

Who has responsibility for the following and their associated procedures:

- key generation
- key issue
- key revocation
- key renewal
- key storage

Provide details/references for any documented key management standards and procedures:

Are any key management products, trusted agents or services used? Please specify

NHS Information Governance

Are certification authority products or services used? Please specify
How are keys stored?
What are the mechanisms for recovering lost keys?
How are keys for backups and archives handled and how is business continuity planning addressed?
Detail the procedures used to verify the trustworthiness of staff involved in key management:
Provide details of any guidance to end-users regarding key management:
Regulatory aspects
Provide details of any regulatory requirements:
Contractual measures
Provide details of any contractual measures taken to support the use of cryptography (for example, to support the use of digital signatures to resolve disputes):
Provide details of any other contractual arrangements with third parties: