

GPSoC Requirements for the Secure Storage and Transmission of Patient Identifiable Data

Amendment History:

Version	Date	Amendment History
V0.1	3 rd April 2008	For approval
V1.0	7 th April 2008	Approved

Forecast Changes:

Anticipated Change	When

Distribution:

Name	Address
GPSoC Suppliers	
SHA and PCT GPSoC Leads	

Document Status:

This is a controlled document.

Whilst this document may be printed, the electronic version maintained in FileCM is the controlled copy. Any printed copies of the document are not controlled.

Related Documents:

These documents will provide additional information.

Ref no	Doc Reference Number	Title	Version
1	NPFIT-SHR-QMS-PRP-0015	Glossary of Terms Consolidated.doc	13

Glossary of Terms:

List any new terms created in this document. Mail the NPO Quality Manager to have these included in the master glossary above [1].

Term	Acronym	Definition

Contents

1	INTRODUCTION	5
2	DEFINITIONS	5
3	REQUIREMENTS.....	6
3.1	ENCRYPTION OF PATIENT IDENTIFIABLE DATA.....	6
3.2	ENCRYPTION KEY MANAGEMENT	7
3.3	TRANSFER OF PATIENT IDENTIFIABLE DATA	7
4	SERVICE DESCRIPTION.....	8

The requirements in this document will be incorporated into an upcoming revision of the Information Governance Foundation Module V2 Baseline Index V1.3, as described in GPSoC-CCN-006 dated 16 November 2008.

1 Introduction

These requirements cover the circumstances where devices or services offered by the Supplier result in the transfer of patient identifiable data through electronic means or by removable media and devices. Examples of removable media and devices to which the requirements apply include but are not limited to: CD, DVD, tape, USB memory stick, removable hard drives, laptops and PDAs.

These requirements also cover where services offered by the Supplier result in the storage of patient identifiable data in insecure environments. Examples of this include servers or desktops in a Practice

NHS Connecting for Health has procured an encryption solution for removable media and full disk encryption for use by the NHS (see Definitions below for reference). The selected product, 'SafeBoot', a McAfee solution, is provided by Trustmarque Solutions. This product is suitable for full encryption of disks and other removable media but does not meet the requirement for encryption of tape backups.

Note that prior to any transfer patient identifiable data taking place, full consideration must be given to the business need for the transfer, and for any opportunity to anonymise the data.

2 Definitions

Secure Courier Services

A Secure Courier Service is considered to be a service which is contracted to the organisation and provides guaranteed secure and acknowledged delivery of media from the sending organisation to a known recipient. This may also include the possibility of this being hand delivered by the Supplier's, PCT's or practice's staff.

Approved Cryptographic Standards sets out the Authority's high level cryptographic algorithm requirements and are contained in the document entitled "Approved Cryptographic Algorithms – Good Practice Guidelines".

The FileCM reference is NPFIT-FNT-TO-IG-GPG-0004.01, and the document is also available at <http://www.connectingforhealth.nhs.uk/infrasec/gpg> or by email request to esp.ig@nhs.net.



acs[1].pdf

Encryption Guidance provides the NHS and NHS CFH suppliers with additional guidelines on the use of encryption to protect patient identifiable and sensitive information. It is available at <https://www.igt.connectingforhealth.nhs.uk/WhatsNewDocuments/Encryption%20Guidance%2031.1.2008.doc>



Encryption Guidance
31.1.2008.doc

NHS Encryption Tool is the encryption solution procured by NHS CFH for use by the NHS. The selected solution from McAfee, 'SafeBoot' is more fully described at the following website : <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/encryptiontool>

VLAN

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location.

3 Requirements

3.1 Encryption of Patient Identifiable Data

The Supplier shall demonstrate that it has limited the patient identifiable data transferred to portable media to the minimum required for the relevant service.

Where devices or services offered by the Supplier result in the transfer of any patient identifiable data on any portable media, encryption shall be used. The level of encryption used shall conform to the Approved Cryptographic Standards.

Where devices or services offered by the Supplier result in the transfer of any patient identifiable data outside the local physical or virtual network (VLAN), including transfers across VLAN boundaries within a single local network or exporting data to removable data, encryption shall be used. The level of encryption used shall conform to the Approved Cryptographic Standards.

The encryption, decryption, transport, storage and destruction of data which is transferred shall be auditable with the media logged and tracked to ensure all instances are accounted for.

The Supplier shall ensure that the encryption product used is accredited to FIPS 140-2 and should have received CCTM accreditation (see http://www.cabinetoffice.gov.uk/csia/claims_tested_mark.aspx).

3.2 Encryption Key Management

The supplier shall ensure that the encryption key for each archive is of an appropriate strength and complexity as detailed in the Approved Cryptographic Standards.

Where encryption keys are generated by the system automatically for transfer of data by portable media, the system shall provide the encryption key to the Data Controller for each encryption operation.

The Supplier shall ensure that any encryption keys generated by the system are stored securely to enable data recovery in the event of key loss or corruption by the Data Controller.

The supplier shall ensure that the encryption key for each archive is unique to that data archive.

Where the Supplier system provides a mechanism for sending encryption keys to a recipient, either electronic or manually, there must be processes in place to ensure that the encryption keys are sent following a separate communication mechanism to the encrypted data or posted separately from the encrypted media.

3.3 Transfer of Patient Identifiable Data

Where a service offered by the Supplier requires the transfer of patient identifiable data by portable media the media shall be encrypted to the level required by the Approved Cryptographic Standards and transported in a secure manner. The transfer of Patient Identifiable Data shall be conducted using Secure Courier services following Department of Health Encryption Guidance guidelines.

Where a service offered by the Supplier requires the transmission of patient identifiable data by electronic means, the data shall be transmitted in an encrypted to the level required by the Approved Cryptographic Standards. This encrypted data can be transmitted via a secure email service such as NHS Mail or over an approved network such as N3.

These services will be included in the GPSOC Framework Agreement by CCN

4 Service Description

The Supplier is required to adhere to the new requirements for the secure storage and transmission of patient identifiable data. These requirements are set out above, and will be reproduced in an update to the **GPSoC IG Specification**, the current version of which is the Information Governance Foundation Module V2 Baseline Index V1.3, as described in GPSoC-CCN-006 dated 16 November 2008.

The following sections set out the information required from the Supplier in respect of new Additional Services and the implications for existing Additional Services under the GPSoC Framework Agreement.

New Additional Services

The Supplier shall supply a description of each of the following services, demonstrating how they meet the requirements set out in the GPSoC IG Specification.

- Encryption of GP clinical IT system back ups at source
- Encryption of data archives on portable devices
- Encryption of data archives exported to other portable electronic media
- Secure Courier Services
- Encryption of drives or desktops using the NHS Encryption Tool

As a minimum the service description shall include:

- Name of GP clinical IT system
- Name of the cryptographic product offered by the Supplier
- The number of practices/systems that will require this upgrade
- A summary of how the supplier intends to manage the encryption keys including
 - Key generation
 - Key issue
 - Key revocation
 - Key renewal
 - Key storage
- A description of how the solution will be implemented including, the option for a PCT or practice to install the cryptographic product or the rationale for precluding this.
- Confirmation that the encryption of data archives on servers and desktops using the NHS Encryption Tool, will not interfere with the normal operation of the GPSoC Services offered by the Supplier.

Existing GPSoC Additional Services

The Supplier shall revise the description of the following existing GPSoC Services and either confirm that these services meet the requirements set out in the GPSoC IG Specification or describe how the existing services will be upgraded to meet these requirements.

- Back up tape verification
- Provision of PDA and laptop supported services
- Data migration
- Any other services offered by the supplier which involve the secure storage or transfer of patient identifiable data