



eHealth Mobile Data Protection Standard

FINAL

September 2008

NHSScotland Mobile Data Protection Standard v1.0

29 September 2008

ehealth.da@scotland.gsi.gov.uk

1. Introduction	3
2. Patient and staff identifiable information security policy	3
3. Responsibilities	3
4. Basic minimum requirements	3
5. Data encryption	5
6-10. Data protection	9
11. Annexe A – FIPS approved product examples	10

1. Introduction

This document describes the minimum standards for the protection of mobile data in NHSScotland. The standard is primarily targeted at laptops and USB memory sticks, however the controls are equally applicable to other mobile data devices such as PDAs, Blackberries and removable media.

1.1 Other relevant standards and policies

This is an NHSScotland standard, it supplements the NHSScotland Information Security Policy and Standards (NHS HDL (2006) 41).

2. Patient and staff identifiable information security policy

NHSScotland policy statement:

Except when specifically authorised after a risk assessment of the necessary business case: patient, staff or other corporate records shall not be stored on mobile devices including laptops, USB memory sticks, PDA's, Blackberries or any other mobile device or media such as smart phones, CD or DVD.

In some cases storing patient information on a mobile device may be unavoidable for the completion of work duties and the provision of care. Such cases shall be subject to:

1. appropriate risk assessment and approval by the local IT security officer;
2. meet the security requirements set out in this document; and
3. be approved by a Caldicott Guardian.

3. Responsibilities

The implementation of these security controls depends on the clear definition and acceptance of responsibilities:

- Scottish Government eHealth Directorate – define the policy and specify the minimum standard;
- Board ITSO – documenting risk management and product selection process, ensures mechanisms in place to adhere to national policy;
- Board Chief Executive – accept and implement the policy, ensure that security controls identified by ITSO are implemented;
- Local IT managers – to deploy the technical security controls agreed with the ITSO.

All responsible individuals are required to sign policy compliance statements on an annual basis.

4. Basic minimum requirements

All mobile data devices should be protected through the application of appropriate security controls regardless of the sensitivity of the information

they are carrying. It is the responsibility of authorities issuing mobile devices to ensure that at least the following security controls are implemented:

- Physical controls
 - the device owner ensures basic physical protection such as keeping the device locked away;
- Technical controls
 - use of appropriate authentication, encryption, and other technical separation controls;
- Procedural controls
 - registration and allocation of an asset to an owner¹ and the maintenance of the register including managed return of devices when an individual leaves post;
 - security operating procedures to minimise the risk of an individual accessing a device for which they are not authorised e.g. by using an unattended laptop, by stealing an unattended USB stick or Blackberry, by over-looking sensitive information on a laptop screen on a train, etc.
- Personnel controls
 - ensuring that only authorised users are issued with a device;
 - ensuring the identity of an individual if you are transferring;
 - establishing clear responsibilities and accountability for the owner of the device regarding processes that must be adhered to;
 - training and awareness for those responsible;
 - ensuring that the responsibilities and accountability are articulated and understood by the data owner i.e. the signing and annual renewal of local compliance statements by all staff.

All asset owners and other individuals with security responsibilities are required to sign local compliance statements renewed on an annual basis detailing their responsibilities with respect to security controls set out in this document.

¹ If devices are allocated on a shared basis, each individual is required to check devices out and sign them back in.

5. Data encryption

The confidentiality of sensitive information that is held on mobile data devices must be protected at rest using the following security controls:

Information type	Examples ²	Security requirements	User access control	Suggested products
Public domain information.	Website extracts. Publicly available information of any sort. (OGC Impact Level 0).	No special security requirements.		N/A

² These categories align to a protective marking scheme that is in development – refined definitions of each category to be finalised

Information type	Examples ²	Security requirements	User access control	Suggested products
<p>Information that is commercially or clinically sensitive and requires a degree of protection, however individuals are not identifiable.</p>	<p>Anonymous patient information. Internally distributed patient statistics or demographic data. Internal memo. Some corporate studies or circulars. (OGC Impact Level 1 and 2).</p>	<p>Encryption: whole disk or file/folder encryption package from a reputable supplier (whole disk preferred). Preferably evaluated to the FIPS 140-2 standard (see last section for examples of FIPS products). The decryption process may be incorporated into the operating system. Challenge – response password recovery is acceptable. Reporting security breaches: loss of devices carrying information, encrypted or otherwise, should be reported to local IT security officers and hospital Chief Executives.</p>	<p>Disclosure Scotland clearance, equivalent to OGC registration level 2. Minimum of single factor authentication e.g. username and password.</p>	<p>Whole disk: BeCrypt DISK Protect Baseline. PGP whole disk encryption. Safeboot. File/folder: PGP file/folder encryption. Windows file encryption, or other file encryption solution. Winzip (v9+).</p>

Information type	Examples ²	Security requirements	User access control	Suggested products
<p>Personally identifiable information or information that is otherwise commercially or medically sensitive.</p> <p>Need to know principle is applicable.</p>	<p>Patient or staff identifiable information.</p> <p>Dental record.</p> <p>Staff performance appraisal.</p> <p>Corporate records containing finance, performance, staff information etc.</p> <p>(OGC Impact Level 3).</p>	<p>Encryption: a CAPS-evaluated whole disk cryptographic product approved to the equivalent of OGC Impact Level 3. Equivalent products to protect stand alone removable media which shall be wholly encrypted.</p> <p>(Local IT security officers may choose to approve the use of a commercially comparable product approved to the FIPS 140-2 standard, based on recorded risk assessment).</p> <p>The decryption process should be separated from the operating system and may be protected by single factor authentication.</p> <p>Reporting security breaches: Loss of devices in this category shall be reported to the Scottish Government.</p>	<p>Disclosure Scotland clearance, equivalent to OGC registration level 2.</p> <p>Minimum of single factor authentication e.g. username and password.</p> <p>Two factor authentication preferred.</p>	<p>Whole disk:</p> <p>BeCrypt DISK Protect Baseline.</p> <p>PGP whole disk encryption.</p> <p>Safeboot.</p> <p>or equivalent product.</p>

Information type	Examples ²	Security requirements	User access control	Suggested products
<p>Information that is more sensitive than patient identifiable information.</p> <p>Need to know principle is applicable.</p>	<p>Information the release of which may undermine confidence in the NHS at a national level.</p> <p>Results of experimental drug trials in certain circumstances.</p> <p>Highly sensitive internal reports for example detailing mis-diagnosis or mis-treatment.</p> <p>(OGC Impact Level 4).</p>	<p>Encryption: a CAPS-evaluated whole disk cryptographic product approved to the equivalent of OGC Impact Level 4. Equivalent products to protect stand alone removable media which shall be wholly encrypted.</p> <p>This typically will be a whole disk encryption solution implemented in hardware or software protected using a password and physical token.</p> <p>The decryption process should be separated from the operating system and shall be protected by dual factor authentication.</p> <p>Reporting security breaches: Loss of devices in this category should be reported to the Scottish Government.</p>	<p>Minimum of two factor authentication e.g. one time password token.</p>	<p>Whole disk:</p> <p>BeCrypt DISK Protect Enhanced.</p> <p>FlagStone Enhanced or Advanced.</p> <p>nCrypt Advanced.</p> <p>or equivalent product.</p>

6. Data protection – laptops

Whole disk encryption shall be applied based on the sensitivity of the information held on the laptop as described in the table in section 5.

Use of file and/or folder encryption for information with low sensitivity shall be accompanied by appropriate procedural controls, and clear allocation of responsibilities.

7. Data protection – additional software controls

Additional security software may be required as determined by the local ITSO, for example:

- USB and port control software (to prevent use of unauthorised devices);
- Enterprise management software to audit usage, location, tampering, etc;
- Standard anti virus and other preventative security software.

8. Data protection – USB memory sticks

Procurement of USB memory sticks should be through trusted and approved procurement routes managed within Boards.

Encrypted USB sticks should be wholly encrypted and not include an accessible unencrypted partition.

Within a given security domain, use of non standard USB sticks should be restricted to ensure that only secure approved USB sticks are used. It is anticipated that selection of approved USB sticks will be undertaken by each Health Board; however, two examples of FIPS140 approved products are provided in Annex A.

All USB sticks shall be assigned an asset number and allocated to an individual who is responsible for managing that device.

9. Data protection – removable media

Export of patient identifiable information onto removable media such as CD, SD cards, DVD or ZIP drives should be avoided. If there is no alternative and the use of removable media in this context has been approved as set out in section 2, the following security controls should be applied:

- The media shall be wholly encrypted using a product such as those set out in the table in section 5. Where whole disk encryption products include the functionality to encrypt removable media this should be applied. Otherwise a suitable equivalent product should be used;
- Transport of removable media containing sensitive information should be only by trusted hand (further guidance TBD).

10. Data protection – device and media disposal

At end of life asset managers are responsible for ensuring that devices and media shall be disposed of or recycled in a secure fashion. Erasure of data shall be carried out using software approved for the removal of information with a government protective marking of RESTRICTED for patient identifiable or generic corporate records. Disposal should be carried out using a service approved to the same government protective marking.

11. Annexe A – FIPS approved product examples

A full reference of FIPS 140-2 approved products can be found at: <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>

Product	Platform	Description
Microsoft BitLocker Drive Encryption	Windows Vista Client	Windows BitLocker Drive Encryption is a data protection feature available in Windows Vista Enterprise and Windows Vista Ultimate for client computers. BitLocker provides enhanced protection against data theft or exposure on computers that are lost or stolen, and more secure data deletion when BitLocker-protected computers are decommissioned.
BlackBerry Cryptographic Kernel	Handheld Device (Blackberry)	The BlackBerry Cryptographic Kernel is the software module that provides the basic cryptographic functionality for the BlackBerry.
IronKey Secure Flash Drive	USB memory stick	The IronKey Secure Flash Drive has been designed to be the world's most secure flash drive. The onboard AES, RSA, SHA, and RNG engines deliver the gold standard in data and identity protection for consumers, enterprises, and government users alike. For more information, visit https://www.ironkey.com .
Kingston S2 CM	USB memory stick	The Kingston S2 CM is the core component of this performance secure USB Flash Drive. All data stored in the users private partition is encrypted in hardware without reducing performance. The Kingston S2 CM provides encryption, user authentication and access control independent of the host software and hardware.
AirFortress® Wireless Security Gateways	WiFi	The AirFortress® Wireless Security Gateways are electronic encryption modules that enforce network access

		rights and encrypt/decrypt communication across a WLAN. Installed by the vendor onto a production-quality hardware platform and deployable on any LAN or WAN, the AirFortress« Wireless Security Gateways provide encryption, data integrity checking, authentication, access control, and data compression.
SafeGuard Cryptographic Engine	Multiple platforms	SafeGuard Cryptographic Engine (SGCE) is a high-performance cryptographic library. It provides cryptographic services to the following products from the SafeGuard solutions: SafeGuard Enterprise, SafeGuard PrivateDisk, SafeGuard LAN Crypt and SafeGuard PrivateCrypto.
Windows CE and Windows Mobile Enhanced Cryptographic Provider (RSAENH)	Mobile Device (Windows CE and Windows Mobile)	Microsoft Windows CE and Windows Mobile Enhanced Cryptographic Provider (RSAENH) is a general-purpose, software-based, cryptographic module for Windows CE and Windows Mobile. It can be dynamically linked into applications by software developers to permit the use of general-purpose cryptography.
PGP Cryptographic SDK	Multiple platforms	The PGP SDK provides all cryptographic and key management functionality for the PGP suite of products, including PGP Desktop Security, PGPnet VPN Client, PGPdisk and the PGP Certificate Server. This is a high-level toolkit for use with C/C++ applications on Windows. It also supports PGP/MIME, TLS, Certificate Server management, LDAP, and Blakely-Shamir Key Splitting, as well as many user interface components for simple integration into other applications. PGP SDK implements only strong cryptography, and the source code is published in book form for peer review.
McAfee Endpoint Encryption for PCs Client	Generic client	McAfee Endpoint Encryption for PCs Client is a high performance software solution that provides sector-level

(formerly SafeBoot Client)		encryption of a PC's hard drive in a manner that is totally transparent to the user. In addition, the centralized McAfee Endpoint Encryption management system provides robust recovery tools, administration, and implementation.
-------------------------------	--	--