Directorate for Health Finance and Information
eHealth Division

The Scottish Government

Dear Colleague

NHSSCOTLAND MOBILE DATA PROTECTION STANDARD

CEL 25 (2012)

10 July 2012

Summary

1. The Mobile Data Protection Standard, first issued in 2008, has now been revised and takes into account the rapid adoption by Boards of new types of device, such as tablets, smart phones and digital pens, for a variety of purposes.

Background

2. The benefits of using portable devices in NHSScotland are massive, ranging from the hand-over of patient notes to colleagues within a hospital, accessing information when meeting patients in their homes, to using a digital pen to send data on a form back to the Board, or simply reading emails remotely. The mobility and flexibility that this brings enhances the quality of care as well as efficiency.

3. The use of portable devices carries with it obvious risks, such as the loss of patient and sensitive business information. NHSScotland, through its Information Assurance Strategy, has already demonstrated its committment to reducing the risks relating to the confidentiality, integrity and availability of the information it holds.

4. This standard sets out the steps that should be taken, such as configuring devices so there is little or no business data held on them, as well as covering matters related to the encryption of data, to ensure that the privacy or business impact of losing a device such as a laptop or removable media is low.

Action

Chief Executives are asked to:

1. Ensure the dissemination and implementation of the revised standards across their organisations.

Yours sincerely

John Matheson
Director, Health Finance and Information

Addresses

For action:
NHS Board Chief Executives

For information:
eHealth Leads
Information Govenance Leads
Information Security Leads
Caldicott Guardians

Enquiries to:
Daniel Beaumont
eHealth Division
St Andrew's House
Regent Road
Edinburgh EH1 3DG

Tel: 0131-244-2770
Email: daniel.beaumont@scotland.gsi.gov.uk

Further copies of this CEL can be downloaded from:
http://www.show.scot.nhs.uk/

NHScotland: Mobile Data Protection Standard

- **Purpose:** this is an updated standard aimed at ensuring minimum technical measures, especially 'data at rest' encryption, are in place where personal and sensitive data are stored on portable devices.

- **Existing investments**: boards are **not** expected to change anything that is already in place to meet the earlier standard (i.e. encrypted laptops). It is aimed primarily where there is a new business requirement (e.g. new portable devices for new applications or replacement of existing devices).

- **Wider risk assessments:** This standard focuses purely on the minimum technical security requirements (Figs 1, 2 and 3) that need to be in place on devices for different categories of information and is designed to be used in conjunction with the Managing Information Assurance for Mobile Wireless Services guidance that looks at the wider issues that need to be considered (and the need for board-level risk assessments before such services are introduced).

Key terms

'Official device' = a device which has been purchased and is controlled by the organisation throughout its lifecycle.

'personally-owned device' = a device which has been purchased by the end-user. The employer may where practicable insist on some controls to be in place (technical or other) before it can be used to connect to a service. And the device may need to be of a certain specification, and have software downloaded onto it, to be able to use an official service.

1. Why the need for an updated mobile data standard?

The original mobile data standard (2008) was written for an ICT environment which was predominantly based on desk-top PCs but with an emerging requirement to access information remotely from mobile devices such as laptop computers and/or to temporarily store information on the hard-drive of a mobile device such as laptop or in the storage memory of removable media (i.e. optical disks, dongles etc). Holding data on such mobile devices poses obvious risks and the standard rightly placed great emphasis on encryption as a means to drastically remove the risks to the data if a device was lost or stolen. An attacker may obtain the device but could either not use it because the whole disk was encrypted (without this 'ignition key' even the operating system could not work) or could not read the data without the keys to open the files therein. A comprehensive approach to encryption (i.e. on all standard issue laptops and all removable media) has until recently been an appropriate and successful strategy given one can never be sure on a daily basis the sensitivity and volume of data that any given user may store on it. And it is almost certain that many privacy breaches in NHSScotland have been prevented as a result.

However, since then there have been considerable changes to technology and to approaches in data handling. Particularly:

- A vast range of new mobile devices such as smart phones, tablets and digital pens that can access and to a greater or lesser degree store data and which alter our traditional perception of what is a 'PC'. Some of these devices may be personally-owned.

- Many of these devices work on short-range wireless and set up to work only ‘on site’. In some senses they could be seen as extensions to desk-top PCs that happen to work without wires. The risks therefore are different from a device which is set up for use at home or on the move.
- New methods to access data, such as virtualisation, can mean that almost no readable data is held on the access device itself as in the past. In such cases encryption for ‘data on the move’ and other measures such as ‘remote wipe features’ maybe more relevant than just relying on encryption for ‘data at rest’.
- A plethora of new eHealth mobile services have been launched which are not all clinical or hold personal data and may not therefore require encryption at all (or encryption of the standard required for the most sensitive clinical data). Feed-back from boards has shown that a less rigid approach to encryption standards is now required (rather than necessarily using those in central government where different military and national security risks apply).
- Although the business requirement for ad-hoc use of removable media such as disks and dongles is waning (as more people can access the data they need remotely) this has brought with it new types of risk. Often storage memory cards within smart phones for example escape the usual encryption process. And the ability to send high volumes of data straight from the device (which in the past could only be downloaded onto an encrypted removable memory drive) means users need to be better aware of how data is categorised in terms of sensitivity and whether it is permissible to hold in such volumes or permissible to transfer it electronically (e.g. via email).
- Now that mobile devices are so pervasive the user education aspects are more important than merely relying on ‘encryption to do security’ as in the past. For example, even if board application is set up so that no data is actually stored onto a personally-owned or official device when a service is accessed (e.g. viewing a clinical record temporarily on screen but not downloading it anywhere) there is nothing that can be done technically to prevent a user from using the device in a way that was not intended (e.g. creating new types of work-related document and storing it on a personally-owned device or finding ways to capture screen shots).

2. What is sensitive information?

All NHS information should be handled with care, especially that which contains personal data. But some types of information are more sensitive than others and this determines whether encryption and other measures needs to be in place.

Higher sensitivity is not determined simply by the type of documents to be held on a device (e.g. x assessment form or Y appointment letter). Instead, a judgement needs to be made as to the impact that would be caused if the information was lost or misused.

Three broad categories or levels can be used to describe the information which the NHS holds. For simplicity these can be viewed like traffic lights: ‘Green’, ‘Amber’ and ‘Red’ (see Annex A).

3. Ensuring there is the right level of technical security for the sensitivity of the data being stored

The following three tables show what **minimum** technical measures, particularly encryption, needs to be in place for devices which hold information of different sensitivity levels (or which connect to applications which hold information at this level).

In some cases the sensitivity of the data that a device is likely to hold will fall squarely in one category (e.g. Amber) but in other cases it is likely to spill into the higher category (Red). The higher category must always be used if there is an expectation of any such material being stored. Decisions must follow an appropriate board risk assessment:

For example:

- An assessment of non-clinical administrative support staff due to be issued with official laptops may show that although the information they routinely handle is unclassified they might expect to occasionally come into contact with sensitive personal data and some corporate data which could cause distress or embarrassment if lost. This would mean therefore that the Amber level technical measures would need to be in place. It may also be easier to maintain a policy decision that all board laptops need to have whole disk encryption as a matter of course than administer a mixed environment for different groups of employees.
- An assessment of a pool of laptops which cannot be connected to the network and used only by external communications for public domain PowerPoint presentations may still identify an unbearable risk of an NHS official putting protected information on there by mistake. Here Amber level may still be appropriate.
- An assessment of smart phones set up for a single purpose (e.g. ward inspection notes) may consider that the data is at protected level but would never go into the highly sensitive level because of the way the devices have been configured. Here Amber level would be appropriate.
- An assessment of smart phones issued to clinicians to access a patient booking system remotely may conclude that although the data held is at protected (Amber) level the volumes of data in question mean that the impact of loss of misuse moves it up to the highly sensitive level. This means Red level technical measures would need to be in place.
- An assessment of digital pens that temporarily store data used by two groups of community nurses who deal with sexual health and maternity issues may show that the type of data is squarely at highly sensitive level (Red).

4. Password strength

It must be stressed that the benefits of having a form of encryption on the data at rest are negated if the password is very weak or if an attacker is given enough attempts to work it out (e.g. users able to carry on using a start-up setting such as 12345 and not being forced to change it). Any encryption product used must be configurable to allow the following:

- At least eight characters long; preferably with at least one number, one special character and one lower and upper case.[1]

[1] This is in accordance with Employee Authentication Management and Single Sign On: Risk assessment and good practice guide for NHSScotland (2012) and NHSScotland Standard Password (2009).

- Password is different from the one used to authenticate onto the network and/or applications.
- A user should be locked out after a maximum of five consecutive attempts where whole disk encryption is used.
- An automatic remote wipe should be considered in the case of smart phones that do not have whole disk encryption after more than ten attempts at password.

Fig 1: Minimum level of technical security required for devices which hold <u>only</u> unclassified information

Note: this assumes that **all** data fits into this category. If there is any likelihood of some data (no matter how small the quantity) being stored at protected level or connected to protected level applications then the amber technical security requirement would apply.

Type of device on which information could be stored GREEN	**Technical security requirements**
Official laptop or tablet[2]	**None** But whole disk encryption still highly recommended as standard for all official laptops as can never be sure what a user will put on it. Only possible exception might for example be a standalone laptop used **only** for public domain presentations.
Official removable media (e.g. dongle, optical disks, digital pens)	**None** But highly recommended for all official removable media to be encrypted as standard. Highly recommended that no un-official (i.e. personally owned) removable media can be used on any official devices.
Official smart phone[3]	**None** But an encryption method still highly recommended as device may be used for multiple purposes. Assess any risks relating to removable media in the device such as SD cards and consider disabling. Consider 'remote wipe' options where reported lost or password attempted ten times.
Personally-owned device	**None** Whole disk encryption currently difficult or impossible to enforce. So steps need to be taken so that no data is stored on the device itself when a service is accessed.

[2] Laptops, notebook PCs, iPads. All of which can be secured with commercially available whole disk encryption.
[3] This is a slightly arbitrary term given the morphing of phones into computers but includes all telephone/messaging devices such as Blackberry and their equivalents which can access and/or store readable information belonging to the organisation. Encryption products can be used other than whole disk.

Fig 2: Minimum level of technical security required for devices which hold up to Amber (protected) information

Type of device on which information could be stored	Technical security requirements
Official laptop or tablet	Whole disk encryption **required**
Official removable media (e.g. dongle, optical disks, digital pens)	Automatic encryption **required** for data put on it Highly recommended that no un-official removable media can be used on any official devices
Official smart phone	Encryption **required** on the data through whole disk or other method unless it can be demonstrated that no personal or sensitive corporate data is stored on the device itself when a service is accessed. Assess any risks relating to removable media in the device such as SD cards. Consider 'remote wipe' options where reported lost or password attempted ten times if whole disk encryption not used.
Personally-owned device	Whole disk encryption currently difficult or impossible to enforce. So steps need to be taken so that no data is stored on the device itself when a service is accessed. Note: NHSmail can currently be set up to allow access from personally-owned devices.

Fig 3: Minimum level of technical security required for devices which hold up to Red (highly sensitive) level information

Type of device on which information could be stored	Technical security requirements
Official laptop or tablet	Whole disk encryption **required**.
Official removable media (e.g. dongle, optical disks, digital pens)	Automatic encryption **required** for any data put on it Highly recommended that no un-official (i.e. personally owned) removable media can be used on any official devices.
Official smart phone	Whole disk encryption **required**[4] unless **only** used to access NHSmail. Assess any risks relating to removable media in the device such as SD cards.
Personally-owned device	Whole disk encryption difficult or impossible to enforce. Personally-owned devices should not be used to store or access information at this level except for access to NHSmail[5].

[4] Products evaluated to FIPS 140-2 standard should be considered where central government originated material marked RESTRICTED is being held but this is not mandatory.

[5] NHSmail is currently the only service set up to allow access via personally-owned devices to information in an email which may be up to Red (highly sensitive/RESTRICTED). NHSScotland eHealth Governance structures will need to consider whether further services become permissible as data partition methods improve

Annex A

Categories of information and impact levels

GREEN: unclassified information

This is information which is unlikely to cause distress to individuals, breach confidence, or cause any financial or other harm to the organisation. This can include information which mentions only a person's name (e.g. routine appointment confirmation letter) as long as it does not contain anything that is judged to describe a person's physical or mental state.

Note: The sensitivity level and impact can also vary depending on the volumes (e.g. a corporate document with just one name of an employee may be unclassified whereas a document with hundreds of names may push it into the amber category below).

AMBER: Protected information

In most boards the largest proportion of patient information can be said to require extra protection because it constitutes sensitive personal data as defined by the Data Protection Act. In particular:

- Any information about an individual (i.e. anything clinical or non-clinical) that would cause short-term distress, inconvenience or significant embarrassment if lost.
- Any information which if lost would lead to a low risk to a person's safety (e.g. loss of an address but no evidence to suggest direct harm would result)
- Any information if lost that would be likely to negatively affect the efficiency of that service (e.g. cancellation of appointments).

RED: Highly sensitive information

Most boards also hold some information which is highly sensitive. Particularly:

- Any information which if lost could directly lead to actual harm (e.g. to mental health or put the person at physical risk from themselves or others in any way).
- Any information that would in the opinion of a qualified person cause substantial distress and/or constitute a substantial breach in privacy (e.g. identity theft, loss of professional standing) to the subject. This is likely to include for example information on a person's sexual health.
- Information that affects the privacy or could cause distress to more than one individual (e.g. several family members or several linked persons contained in a file).
- Information relating to vulnerable persons' health (e.g. child protection cases).
- Information governed by legislation that requires additional layers of security and recognises the substantial distress that would be caused by loss (e.g. embryology, human fertilisation and gender re-assignment).
- Information if lost that is likely to result in undermining confidence in the service or would cause significant financial loss to the organisation, prejudice investigation of crime etc.

Frequently asked questions on revised Mobile Data Protection Standard

1) Why is there a need for this standard?

Portable devices are generally more susceptible to theft, loss and misuse than desk-top PCs. One of the most effective technical controls is to encrypt the data while it is 'at rest' on the device so that it is extremely difficult for any un-authorised person to read the information without knowing the 'key'. Another, is to ensure that little or no readable business data is stored on the device in the first place. This means that although we can never prevent all laptops and similar devices being lost we can greatly reduce the impact (i.e. there is a financial cost for replacing the device and information may need to be re-constructed but no loss of confidentiality).

This standard focuses purely on a narrow set of technical controls.[6] The aim is to get some minimum bench-mark across boards in NHSScotland. It is to be used in conjunction with the wider guidance on deploying mobile wireless devices.

2) Does this revised standard mean I need to change what was put in place since 2008?

No, the revised standard builds on the original 2008 version and relates to where new types of device and services are planned. Boards have invested in whole disk encryption products for laptops and the security benefits will continue to be accrued for as long as the chosen products are operational. The revised standard takes into account smart phones, tablets and emerging devices which carry a new set of challenges compared to traditional laptops.

3) Does the revised standard have any big cost implications?

Much of what is in the 2008 standard is unchanged (i.e. laptops and whole disk encryption) and boards will have taken this requirement into account when replacing existing hardware. The revised standard affects new services/types of device and many of the features required for tablets and smart phones are being incorporated into enterprise versions. The traffic light approach, which is based on business impact, means that for smart phones there is more emphasis on how the application is accessed. And there is no insistence on using one particular product or technical standard.

It must also be stressed to management boards that the financial and reputational cost of not putting in such measures are significant if there is a serious privacy breach. Recent fines relating to loss of unencrypted sensitive personal data relating to health and social care in the UK have been up to £380,000 in 2011/12. And this is of course in addition to the harm and distress that might be caused to individuals.

[6] Other controls, procedural/training and environmental can be found in the NHSScotland Managing Information Assurance for Mobile Wireless Guidance (2012).

4) What are considered to be the biggest threats and vulnerabilities in regard to information held on portable devices in NHSScotland at the moment?

The most obvious and widespread threat is still theft of devices for their monetary value (especially as boards are switching to more desirable tools such as tablets and smart phones). They can also be used for criminal acts (i.e. malicious activity online). A growing threat is persons wishing to target specific public sector staff to obtain personal data in bulk (e.g. names, residential and email addresses which are bought and sold online) or particularly sensitive data which only health professionals might have. Stealing a portable device from staff who are known to routinely handle such information could, in the eyes of the criminal, yield the type of information required (e.g. a GP practice manager may maintain the list of patients in an area on spread sheets; so it might be assumed that stealing the laptop is a way of getting such bulk data; or stealing a tablet from a parked car used by a social worker on visits might in all probability hold sensitive details on families in a given area).

If such NHSScotland devices are encrypted as a matter of course (or hold no data or have features that render the device useless) then as well as reducing the impact of loss it can also dent the motivation of criminals to carry out future acts (i.e. “no point stealing NHSScotland devices as you cannot do anything with them without a lot of effort”).

The other significant risk still relates to removable storage media. Although organisations have invested in procuring encrypted dongles that hold patient or sensitive corporate data some other vulnerabilities have been overlooked. For example allowing someone to plug in an un-official or personally-owned dongle or smart phone into an official device’s USB, means malware such as key logging software or viruses can be easily spread across the whole network and remain un-detected. This was the method used to spread the Stuxnet worm for example which went undetected for years. And often smart phones are set up so that no data is stored on the encrypted internal memory but then external memory such as SD cards can be used, inserted and removed and have no form of protection.

5) Why is password protection not enough?

There is a fundamental difference between ‘password protection’ and an encryption method which happens to use a password as a ‘key’. Laptops and similar devices stolen from NHS organisations with just password protection are to all intents and purposes considered as having virtually no protection and certainly not enough to prove adequacy for seventh principle of the Data Protection Act.[7]

A password, if not encrypted, is relatively easy to crack on a mobile device within a short space of time. And there are often ways to circumvent putting in a password which might be required to run the operating system but still get at the data.

Encryption software by contrast makes it extremely difficult to find the key that will unlock the data itself and most attackers would not have the time or resources.

[7] Laptops containing data on thousands on individuals were stolen from NHS North Central London (June 2011); in mitigation the trust said that there was ‘password protection’ but in the eyes of ICO and security professionals this constituted virtually zero protection and certainly not adequate enough to satisfy seventh principal of Data Protection Act.

6) What is meant by whole or full disk encryption?

The device itself can be switched on but it cannot be booted up or used in anyway unless the 'key' is inputted.

This is the most comprehensive form of encryption on a device as it means that an attacker cannot simply take out key components (e.g. memory drives) and recover the data.

The massive benefit of this type of encryption over other forms is that you do not need to second guess what a user may or may not put on any segment of the device's memory throughout its life-cycle. What ever data is held on it is secure unless the attacker knows the key.

7) When must whole disk encryption be used and why?

For information deemed highly sensitive ('red')[8] then whole disk encryption must be used for all laptops, tablets and smart phones. This is because the impact of the loss of information at this level could be significant and measures need to be taken to ensure that any information put onto the device (by design or accident) are protected. The only current exception to this rule is if emails are being accessed via NHSmail or other approved services (see below) because special measures are in place. Thus if the device, including a personally-owned device, is not being used for any 'red' level material other than what might be accessed on NHSmail then whole disk encryption is not mandatory.

8) What do I do about devices that hold patient information at the 'amber' or lower end of sensitivity?

In the case of laptops and tablets whole disk encryption is still required for information at this level. This is because these devices can be used just like desk-top PCs and there is great potential for the user to store a greater range and higher volumes of data (wittingly or unwittingly) than phones.

But for smart phones there is more flexibility if they are to be used only up to 'amber level. A board can either a) chose to put in whole disk encryption just like laptops and tablets or b) configure the service in such a way that the devices do not hold any NHS information in order to access and operate a service or use an encryption method that protects the segment holding business data. This flexibility clause recognises the technical developments in the smart phone software area which can lessen the need for whole disk encryption.

There are still risks associated with this approach (e.g. a user putting 'amber' business information onto an application or segment of the device by mistake that is not encrypted) or an application which purports to hold no data on the device turns out to cache some data for varying periods (e.g. calendars, contacts, data waiting for network coverage in order to be synchronised). Such issues need to be considered as part of the board's risk assessment.

[8] This is broadly equivalent to RESTRICTED material in HMG.

9) How do I get whole disk encryption on such a range of devices?

Putting whole disk encryption on laptops is now well established since the last mobile data standard (2008) and there are many products available. Until recently getting such encryption on other devices has been more problematic with fewer commercially available solutions. But this is fast changing and many of the devices now have a form of on-board whole disk encryption (e.g. last two releases of ipad and some Android devices) that can either be enabled or work out of the box. It should be stressed that such on-board solutions are adequate for NHSScotland requirements.[9] There are also third party end-point security solutions which can be added to smart phones.

When considering the cost of getting devices that can achieve the effect of whole disk encryption it is useful to discuss again with the customer the type of device that is most appropriate for the purpose: is the eHealth service best accessed and information captured or updated via a smart phone or a tablet? And do the benefits of using one type of device outweigh the higher costs incurred in getting whole disk encryption in place? (i.e. often getting whole disk type encryption solution on smart phones can be more difficult and costly than on a tablet where it may be out of the box).

10) Are there any particular products and technical standards for whole disk encryption that must be used?

No. A board can choose to use any product it judges as long as the outcome is the same. In the case of technical standards FIPS-140-2 products are becoming more readily available and might be needed where information marked RESTRICTED is to be routinely shared between NHSScotland and central government over a long period. For example future projects relating to child protection, crime and emergency planning might need FIPS-140-2 and other technical controls before partners agree to share information that might be accessed via portable devices. But ultimately it is a board-level decision as to whether to get compliance to this particular technical standard.

11) What do we do about personally owned devices?

The mobile data standard assumes that it is currently extremely difficult or impossible to attempt to put in the same measures that you would for official devices.

For this reason personally owned devices **must not** be used to process any NHSScotland data which is highly sensitive (‘red’) except for NHSmail. Other exceptions can be reviewed by the governance structures of NHSScotland.

In the case of ‘amber’ level information personally owned devices can be considered but must be set up so that no data is stored on the device when a service is accessed and a remote wipe function should be considered for any residual data.

[9] Although not all of these on-board whole disk solutions may meet UK military, national security and some HMG requirements they are adequate for NHSScotland.

This is an emerging area and needs to be handled with great caution. For example can you be sure that the information accessed as part of the service will always be at ‘amber’ level? Can you prevent a user via technical means from accessing the service if they have not followed the steps required such as downloading software? And would the user need to physically bring in the device into the board’s IT department to have it configured or can it be done remotely? Would the support costs of doing this be higher than just issuing an official device that the user would find acceptable (e.g. ipads, Android tablet models that are popular with consumers etc)?

12) What about removable media?

All removable media holding ‘amber’ or ‘red’ level information must be encrypted. And it is highly recommended that all removable media such as dongles and optical disks should be encrypted as a matter of course as you can never be sure what a user will put on it. Furthermore, it is highly recommended that no un-official or personally owned removable media is ever plugged into NHSScotland devices (regardless of whether it is encrypted or not). Apart from the obvious need to prevent the spread of malware, using only official removable media gives the organisation greater control over its assets (i.e. inventories showing what media has been issued to staff, its location and purpose). And there is a general need to greatly reduce the use of removable media in the first place. Often an employee puts data onto a disk or dongle to get over a short term problem (e.g. how do I deliver my large spread sheet to the auditors?). Each board information Security Officer can recommend the most appropriate mechanism to share data in bulk with business partners which might not be via removable media but a secure file sharing protocol for example.

13) What about unclassified information?

For unclassified information there are no mandatory technical requirements. However, a board risk assessment may conclude that it is impossible to always be sure what a device will be used for throughout its life-cycle so that ‘amber’ level measures need to be in place as a minimum.

The only possible type of exception might be a designated pool of devices only ever used for Powerpoint-type presentations. But even here it needs to be borne in mind that unclassified information is not necessarily ‘public’ information and may be subject to Freedom of Information Act Scotland exemptions (e.g. work in progress due to be published next month). The potential reputational damage caused by a member of the public finding *any* NHSScotland information on a laptop might mean it is simpler to just have whole disk encryption as a matter of course.

14) Why are devices which only handle email treated differently?

The way email is treated does at first appear out of kilter with the logic since the information in an email could be highly sensitive and could find its way onto the storage memory of the device like any other business information.

Email is a special case. It is the only business application in NHSScotland which can be accessed on a device without always having the usual data at rest encryption. The reason for this is partly historical: email services via a Blackberry device for example have grown up over the past decade in relative isolation and there have been measures in place to ensure that little or no data was stored on the device itself (i.e. the focus has always been on encryption for data on the move and/or remote wipe). And NHSmail, which is used by some boards in NHSScotland, allows personally owned devices to be used to access the service providing the user downloads some software that creates an encrypted two-way tunnel to the mail server and the means to remotely wipe residual data. There are still some serious concerns with this approach (e.g. remote wipe only has value if you are told promptly when an employee has left the organisation and there are means to circumvent the technical steps required to access the service).

Such points will be considered as part of the NHSScotland email replacement project.