Saskatoon Health Region	**POLICY** Number: 7311-25-007 Title: Security of Mobile Devices and Removable Media
Authorization [ ] President and CEO [X] Vice President, Finance and Administration	Source: Director, Information Technology Services Cross Index: Date Approved: August 10, 2012 Date Revised: Date Effective: August 24, 2012 Date Reaffirmed: Scope: SHR & Affiliates

Any PRINTED version of this document is only accurate up to the date of printing. Saskatoon Health Region (SHR) cannot guarantee the currency or accuracy of any printed policy. Always refer to the Policies and Procedures site for the most current versions of documents in effect. SHR accepts no responsibility for use of this material by any person or organization not associated with SHR. No part of this document may be reproduced in any form for publication without permission of SHR.

Overview

Mobile computing carries the risks of working in an unprotected environment and these risks need to be considered and appropriate protection applied. Mobile computing and communication devices (mobile devices) and removable media such as USB flash drives are common fixtures in the office environment. These technological tools have become indispensable because they offer increasingly large capacity in fast, easy to use, compact, portable formats; in short, they are convenient.

This convenience bears with it some associated risks. Mobile devices are easy to steal and easy to misplace. If removable media goes missing it is more than likely that the data it contains has also gone missing. Privacy breaches of confidential information can also occur as a result of utilizing unsecured wireless networks. Privacy breaches of any sort can have far-reaching implications depending on the nature of the information compromised and the number of individuals affected.

Definitions

SHR User means a person with an active SHR User Account that allows access to the SHR computer network. A SHR User may include SHR employees, affiliate employees, physicians, other health care professionals, students, contractors, vendors and any other person who has been approved for an SHR User Account.

SHR User Account means a personal account consisting of an Active Directory username and a password that is granted for user access privileges, as specified on the *SHR User Account Application Form*. Privileges may include access to shared files, email and/or systems/applications.

SHR User account activity means being logged onto the SHR network, by either direct/internal login or via remote access, using a computer or mobile device, in order to access SHR systems/applications and network resources.

Mobile Device means a laptop computer or a pocket-sized computing device (a device typically having a display screen with touch input or a miniature keyboard that can store electronic data files and software). A mobile device includes, but is not limited to: laptop computer, tablet computer, Palm Pilot, personal digital assistant (PDA), cellular phone, smart phone, and ultra-mobile PC (UMPC). *This includes home PCs and personal mobile devices used to access SHR's network, data, or applications.*

Removable Media means storage media that can store electronic data files or software and be removed from its device reader. Removable media includes, but is not limited to: memory cards, USB flash drives, pens that digitally record data, CDROMs, DVDs, or data backup or storage tapes.

Remote Access means communication to a network using a mobile device from a remote location or facility through a data link (Internet or modem). Some of the more common methods of providing this type of remote access are: remote dial-in through a modem, Citrix login through the Internet, Outlook Web Access and remote email/calendar synchronization via the cellular network through ActiveSync.

Physical Control means to physically secure a mobile device from the risk of theft. Such security includes, but is not limited to: locking it in a drawer or office, using a locking cable to secure it to a desk, equipping with an audible alarm, etc.

Personal Health Information (PHI) means[1], with respect to an individual, whether living or deceased:

- information with respect to the physical or mental health of the individual;
- information with respect to any health service provided to the individual;
- information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
- information that is collected:
    - in the course of providing health services to the individual; or
    - incidentally to the provision of health services to the individual; or
- registration information

1. PURPOSE

The purpose of this policy is to:

1.1 Establish standards, responsibilities and restrictions for SHR users who require access to corporate data from a mobile device. This policy establishes the requirements for safe and secure usage of any such device, whether it is connecting to the SHR network, connecting to any network outside the control of SHR ITS, or used on a stand-alone basis.

1.2 Establish requirements for safe usage and secure storage of removable media used to store or transport corporate data classified as internal or confidential.

[1] HIPA Section 2 (m)

2. PRINCIPLES

2.1 SHR is committed to conducting healthcare with integrity and in compliance with all applicable laws and legislation.

2.2 SHR has a responsibility for the security of the SHR network, resources, systems/applications and information, and for the protection of these assets from potential harm.

2.3 The risk of a security breach can be reduced through prevention and by following the recommended security measures and controls.

3. POLICY

3.1 The SHR Mobile Device Security policy shall apply to, but is not limited to:

3.1.1 All mobile devices and removable media storing SHR data classified as 'internal'[2] or 'confidential'[3]. For a full definition of SHR's information classification categories (and the precautions required to protect each classification) refer to SHR's Information Classification, Labeling and Handling policy.

3.1.2 All mobile devices connecting to SHR's network or any network outside of SHR's network, even if the said equipment is not corporately sanctioned, owned, or supplied by SHR.

3.2 Access Control

3.2.1 Access to the SHR computer network using a mobile device through a network outside of SHR's direct control shall only be initiated for SHR related business use and communication.

3.2.2 SHR users who require remote access to information systems from a mobile device shall request such access as per current ITS policy and procedures regarding remote access to information systems. (Refer to the "Policies & Procedures", "Forms", "Frequently Asked Questions", and "Self Help" sections of the ITS InfoNet for current information.)

3.2.3 ITS reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure. ITS will engage in such action if equipment is being used in such a way that puts SHR's systems, data, users, and clients at risk.

3.2.4 SHR users who wish to utilize personal devices to gain access to SHR data via non-corporate network infrastructure **must employ**, for their devices and related infrastructure, **all** security measures deemed necessary by the ITS department. This includes a personal firewall, a system with up to date operating system patches and virus scanner, and (as applicable) a home

[2] Any information other than PHI that is not classified by the information owner will be assumed to be "Internal" and will be protected with the necessary measures.

[3] All personal health information (PHI) will be assumed "Confidential" and protected with the necessary measures.

wireless network that is encrypted to acceptable levels. This also includes an absence of software (e.g. file sharing programs) that in ITS' opinion unacceptably compromises the security of a user's personal device. Enterprise data is not to be accessed on any hardware that fails to meet SHR's established enterprise IT security standards. (For a list of these standards, please see the ITS InfoNet or consult the ITS Service Desk.)

3.2.5 All mobile devices attempting to connect to the corporate network through an unsecure network (i.e. the Internet) will be inspected using technology centrally managed by the ITS department. Devices that are not in compliance with ITS security policies, or represent any threat to the corporate network or data, will not be allowed to connect.

3.3 Unacceptable Use

3.3.1 SHR Users shall never:

- Permanently store SHR information on a mobile device or removable media. This information must be saved to the network and permanently removed from the mobile device or media as soon as possible.

- Transmit confidential SHR data or PHI over an insecure network where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to SHR's public image. This includes emailing PHI outside of SHR's internal network. (Refer to SHR's Emailing Personal Health Information policy for full details.)

- Make modifications, disable or tamper with SHR owned and installed hardware or software configurations. This includes, but is not limited to: data encryption, screen-saver passwords and anti-virus software.

- Install any software on SHR mobile devices without prior authorization.

3.4 Privacy and Confidentiality

3.4.1 All information stored on SHR, non-SHR or personal mobile devices that has been acquired via the SHR network is the property of SHR. This includes:

- SHR email

- SHR information that would normally be classified as Internal or Confidential. (For guidance, refer to SHR's Information Classification, Labelling, and Handling policy.)

- PHI, including patient appointment information, that is stored in an individual's personal calendar on that device.

- Audit records that may exist that document the mobile device's connections to SHR's network, applications, or services, including all user activity information exchanges that occurred during those connections.

3.5 Security

3.5.1 Addition of new hardware, software, and/or related components to provide additional mobile device connectivity and security will be managed at the sole discretion of ITS.

3.5.2 Non-sanctioned use of mobile devices to back up, store, and otherwise access SHR-related data is strictly forbidden.

3.5.3 Connectivity of all mobile devices will be centrally managed by ITS and will utilize authentication and strong encryption measures.

3.5.4 Any mobile device or removable media that is being used to store SHR data must adhere to the ITS department's authentication and encryption requirements. In addition, all hardware security configurations (personal or SHR owned) not on the ITS list of officially supported IT security standards must be pre-approved by ITS. When in doubt, please consult the ITS Service Desk.

3.5.5 Users of USB flash drives are required to follow SHR guidelines for proper USB flash drive use as listed in Appendix A.

3.5.6 ITS will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass security implementation will be deemed an intrusion attempt and may result in disciplinary action.

3.5.7 This policy is complementary to any other policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the enterprise network.

3.5.8 ITS reserves the right to examine non-SHR mobile devices used to conduct SHR business to determine if they are suitably secure.

3.5.9 If SHR deems their data security to be at risk, SHR reserves the right to:

- Remotely or locally wipe mobile devices or removable media of all data (in some cases, restoring a device to its default factory settings) and/or
- Lock mobile devices or removable media to prevent access by anyone other than ITS.

In some cases, these actions may need to be performed without informing the affected user(s).

In case of loss or theft, the decision to take these actions may be made by IT Security. In situations other than this, consultation with the Director or VP of SHR ITS is required.

3.5.10 By accessing SHR resources on personal or non-SHR phones, non-SHR mobile devices or removable media, SHR Users acknowledge that SHR reserves the right to wipe the device or media clean if the SHR data stored on the device is at risk. Recovery of the device and personal data on the device is up to the user and SHR is not responsible or liable.

3.6 Replacement Costs

SHR Users are responsible for the security of the mobile devices assigned to them. If a SHR-owned mobile device or removable media is lost or stolen:

3.6.1 SHR may pay for a replacement for a particular SHR User for the first occurrence of loss or theft after an investigation to rule out negligence. Whether or not the SHR User's actions constitute negligence will be determined by their Manager based on the physical security principles set forth in this policy.

3.6.2 In the case of negligence, or of any subsequent losses or thefts, the SHR User's out-of-scope (OOS) supervisor may require the User to reimburse the business unit for the replacement costs.

4. ROLES AND RESPONSIBILITIES

4.1 SHR Users shall:

4.1.1 Secure and protect mobile devices and removable media, including SHR information and SHR systems stored on a device and/or that can be accessed from the device. This includes following the guidelines for proper use of USB flash drives as listed in Appendix A.

4.1.2 Read and comply with this policy, all other applicable SHR policy, and all other applicable federal and provincial legislation.

4.1.3 Ensure that all security protocols normally used in the management of data on a SHR network computer are also applied, without exception, when using a mobile devices and related software for network and data access.

4.1.4 Manage remote access according to established SHR IT standards.

4.1.5 Manage all passwords according to SHR's Password Policy.

4.1.6 Protect removable media, whether they are SHR or personal, and all data stored on them by using only SHR ITS-approved encryption security.

4.1.7 Employ reasonable physical security measures for any mobile device used for SHR business, especially when they contain SHR data. This applies whether or not the devices are actually in use and/or being carried. This includes, but is not limited to passwords, encryption, and physical control of such devices (e.g. securing laptops at workstations or in offices with a cable lock).

4.1.8 Return SHR mobile devices to a manager/director/supervisor or designate when no longer needed or when leaving SHR's employ. Non-SHR devices that no longer require access to SHR'S network, applications or data must be wiped clean and/or reset to factory settings. If uncertain on how to do this, contact ITS for assistance.

4.1.9 Immediately report lost or stolen mobile devices or removable media to their Manager and ITS (see procedure 1.4).

4.1.10 Immediately report any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc. to their Manager.

4.2 Managers

4.2.1 Ensure that suitable protection and arrangements are in place for their employees who are required to use a mobile device.

4.2.2 Ensure staff have read this policy and any other policies regarding remote access to SHR's network, applications, and/or data prior to being provided with a mobile device.

4.2.3 Immediately report lost or stolen mobile devices or removable media to the ITS Service Desk. The ITS Service Desk will inform and engage IT Security.

4.2.4 Act on non-compliance or breach of this policy and report such incidents to IT Security.

4.2.5 Return devices no longer required for work assignments within the department they were procured for to ITS Deployment so that a complete data wipe can be performed.

4.2.6 Promptly inform IT Security when an employee or contractor has left SHR's employ so that this person's ActiveSync and/or Webmail access can be removed in a timely manner.

4.3 ITS

4.3.1 Protect the confidentiality, integrity, and availability of SHR information and information systems.

4.3.2 Manage and control access of mobile devices connecting to the SHR network.

4.3.3 Work with IT Security to act on non-compliance.

4.3.4 Monitor all activity and traffic on the SHR network, including any mobile device attempting to connect to the corporate network through an unsecure network (i.e. the Internet), using technology centrally managed by the ITS department.

4.3.5 Investigate inappropriate or illegal activity on the SHR network and report the findings to an ITS Manager. As required, ITS Managers shall involve or inform additional parties such as Privacy & Compliance, People & Partnerships, and the associated user's manager.

4.3.6 Maintain, update and apply configurations to SHR-managed mobile devices in order to provide up-to-date protection features to secure local information.

4.3.7 Keep a register of SHR-managed mobile devices in use with details of owners and installed software.

4.3.8 Support sanctioned hardware and software, but not be responsible or accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software.

4.3.9 Reserve the right to:

- Limit the ability of end users to transfer data to and from specific resources on the enterprise network through policy enforcement and any other means it deems necessary.
- Impose encryption software on all infrastructure end points. This includes but is not limited to, removable USB flash drives, CD/DVD's and mobile devices.

5. POLICY MANAGEMENT

The management of this policy including policy education, monitoring, implementation and amendment is the responsibility of the Director, Information Technology Services.

6. NON-COMPLIANCE/BREACH

Non-compliance with this policy will result in a review of the incident. A review for non-compliance may result in disciplinary action, up to and including termination of employment and/or privileges with SHR.

Violations of this policy will be adjudicated according to established SHR policies and procedures.

- If SHR discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, information stored on mobile devices or removable media may be used to investigate the activity in accordance with due process. Such investigations may require access to information on personal devices or media if those devices/media were used (or suspected to have been used) to conduct SHR business.

- ITS is not able to directly manage external devices which may require connectivity to the corporate network. Therefore, end users must adhere to the same security protocols when connected to SHR information system resources using non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

Sanctions for violations may include, but are not limited to, one or more of the following:

- Temporary or permanent loss of privileges for access to some or all computing and networking resources and facilities.

- Disciplinary action by the manager, in consultation with Labour Relations and according to applicable SHR policies, up to and including termination of employment.

- Legal action according to applicable federal and provincial laws and contractual agreements.

7. REFERENCES

Best Practices. Mobile Device Security. May 27, 2009. Office of the Information & Privacy Commissioner of Saskatchewan Website: http://www.oipc.sk.ca

SHR User Account Policy
SHR's Password Policy
SHR's Information Classification, Labelling, and Handling policy
SHR's Email Acceptable Use policy
SHR's Emailing Personal Health Information policy

For further information on *The Health Information Protection Act (HIPA)* or *The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP)*, please contact Privacy or visit the Saskatoon Health Region's website at http://www.saskatoonhealthregion.ca/about_us/privacy_access.htm

PROCEDURE

Number: 7311-25-007
Title: Security of Mobile Devices and Removable Media

Authorization [ ] President and CEO [X] Vice President, Finance and Administration	Source: Director, Information Technology Services Cross Index: Date Approved: August 10, 2012 Date Revised: Date Effective: August 24, 2012 Date Reaffirmed: Cross Index: Scope: SHR & Affiliates

1. PROCEDURE

1.1 Access Control

1.1.1 SHR Users

- Shall request access as per *current SHR ITS procedures* if they require remote access to SHR information systems from a mobile device. (See the SHR User Account Policy for further details.)

  - o Download and submit duly-authorized forms that reflect the type(s) of remote access required:

    - ▪ For ActiveSync access (from smart phones), submit the ActiveSync Access Application form

    - ▪ For Webmail access (i.e. other mobile devices), submit an Application for Webmail Access

  Both forms are available on the “Forms” page of the ITS InfoNet.

- Register a device with ITS prior to directly connecting to the corporate network or related infrastructure.

- Contact the ITS Service desk at Information Technology Services - Service Desk or 655-8200 (or 1-866-431-1780 from the rural areas) if your preferred USB flash drive does not appear on the list of approved standards.

- **Must employ**, for their devices and related infrastructure, a company-approved personal firewall, up-to-date anti-virus software, and any other security measure deemed necessary by the ITS department, in order to connect such devices to non-corporate network infrastructure to gain access to enterprise data. (For a list of these standards, please see the ITS InfoNet or consult the ITS Service Desk.)

1.1.2 Managers

Ensure that suitable protection and arrangements are in place for their employees who are required to use a mobile device as documented as part of this policy and as published on the ITS InfoNet. (For a list of these standards, please see the ITS InfoNet or consult the ITS Service Desk.)

1.1.3 ITS

- Will deny connectivity to devices if they:
  - Are not in compliance with ITS security policies and standards;
  - Represent any threat to the corporate network or data.

1.2 Decommissioning Mobile Devices and Removable Media

1.2.1 All SHR-managed mobile devices should be returned to the ITS Deployment Team at the end of their lifecycle or prior to being redeployed to another employee for a complete data wipe.

To do this, download and complete an IT Work Order Request Form (available on the "Forms" page of the ITS InfoNet). Clearly indicate "FOR DISPOSAL" or "FOR DATA WIPE BEFORE INTERNAL REDEPLOYMENT", as appropriate.

The ITS Deployment & Break-Fix Team will arrange with the department to have for the IT asset picked up or shipped.

1.2.2 Outdated or defective removable media should be taken to ITS for a complete data wipe. (Refer to the SHR policy *Disposal of IT Assets* for details.) Never dispose of removable media through office or public waste baskets, as confidential data may still be retrievable even if the media no longer appears to be functional.

1.3 Usage Guidelines

The following guidelines are designed to ensure that mobile devices and removable media used outside the office environment are afforded similar levels of protection as equipment and information that is used exclusively within the office environment. This also extends to information processed exclusively within a SHR User's home.

1.3.1 General

- Any unique usage and security awareness needs must be communicated to ITS so these can be addressed.

- Take good care of mobile devices and removable media to prevent accidental damage, such as rough handling, accidentally spilling beverages on the equipment, or being in close proximity to extreme temperature.

- Store all SHR materials, such as data, documents, e-mail messages, spreadsheets, databases, programs, etc. that were received, created or edited on mobile devices in the course of carrying out SHR business on the SHR network. The use of network storage devices will provide for recovery of such materials in the case of loss***. It is strongly encouraged not to store copies of such materials on mobile devices, including removable media, unless necessary.*** Storing materials on such devices exposes information and information systems to disclosure or unrecoverable loss.

  - Utilizing external cloud storage (online file storage space hosted by third parties), calendar services, or other productivity products where storage is outside of SHR's control is not allowed. The security of those services cannot be guaranteed and information stored via these external services may either travel or be stored in the United States of America, making PHI accessible to the American government through legislation such as the USA PATRIOT Act.

- SHR takes a strong stance against software piracy. All third party software installed on mobile devices must be licensed for such usage.

- All external email, software or documents will be checked for viruses before being loaded onto mobile devices.

- Only SHR owned and managed mobile devices or approved devices from select partner organizations (as approved by the ITS department's Vice President) will be allowed to directly connect to SHR's network. Personal laptop computers, UMPC's and PCs may only access the corporate network and data indirectly through mechanisms such as Citrix and Outlook Web Access.

- Smart mobile devices such as Pocket PC's, smart phones, and PDAs will access the corporate network and data using ActiveSync.

1.3.2 Texting and Instant Messaging

Texting is not at as inherently secure as alternative communication modes.

- Some texting companies send information over unencrypted lines to non-secure servers.

- Text messages may subpoenaed if a patient ends up in court and an attorney wants to see text-based interactions with that patient.

- If a smart phone is stolen, the patient's information including phone number may be compromised by a hacker or released to parties outside of that patient's circle of care.

As a general rule, don't send texts containing PHI. If this must be done in an emergency situation, the same care must be taken when texting PHI as when emailing it. This includes:

- Considering if there is another more secure or reliable mechanism that can be used. When in doubt, revert to safer modes of communication.

- Keeping a record of the patient/client/resident's health information or care decisions contained in a texting exchange by adding suitable notes to a SHR clinical application or copying the texts and placing them in the patient's permanent record. Soft (electronic) copies of texts, when deemed necessary, should be stored in an organized manner on a network drive.

- Deleting texts immediately when the information is not required and/or once texts have been stored elsewhere (see above).

For further guidance, refer to SHR's Emailing Personal Health Information policy.

1.3.3 Securing Personal Health Information (PHI)

- Ensure all PHI is de-identified as much as possible for the intended application.

- Consider alternatives to storing PHI on your mobile device. Remotely accessing needed information via a protected remote connection (i.e. secure websites, Virtual Private Networks) is a more secure alternative than storing it locally.

- Remove as few records containing PHI as possible. Instead of accessing the entire database, take only the subset of records/data that you need.

- All smart phones shall be set to lock themselves after a period of inactivity so that a password is required to get in. (All devices that synchronize with SHR email accounts are remotely configured to do this by default.) If this cannot be done with one's device, it may be unwise to store this type of information on your device.

- Anything that can compromise patient privacy (address book entries, email, calendar, text messages) shall be stored on smart phones in an encrypted manner. (See your device's user manual, or contact your service provider, for instructions on how to do this on specific devices.) Most modern smart phones have this capability, it just may not be turned on by default.

- When personal devices (PDAs, smart phones, etc.) are discarded or recycled, they shall be reliably cleansed of any personal health information, including stored records of text message communications. This may require expert assistance, as simply doing a "delete" may not suffice.

- When no longer required, remove PHI from your mobile device as soon as practical. Deleting data files from the screen of a mobile device won't necessarily delete the data completely. Ensure that you empty the device's 'Recycle Bin' or 'Trash'.

1.3.4 Physical Security

- If you must use a mobile device in a public place, make sure that others cannot see your work, and never process sensitive material under these circumstances.

- Know where your mobile devices or removable media are at all times. When not in use or kept on your person, store mobile devices in a secure, locked enclosure or physical control.

  - Never leave mobile devices or removable media unattended, especially in a public place or when traveling. Be particularly vigilant on public transportation and in public places such as stations, airports, restaurants and hotels.

  - Do not leave mobile devices or removable media unattended in your vehicle. If it absolutely cannot be avoided, lock them in the trunk of the vehicle. ***If the vehicle has no trunk, leaving the device in the vehicle is not a secure option.***

  - Laptops at workstations or in offices should be secured using a cable lock.

- Use a non-descript lockable briefcase or laptop case that does not bear any visible logos of your organization or of the device manufacturer.

1.3.5 Taking Your Mobile Computer out of Country

Before taking your mobile device out of country, you should ensure that is not storing any PHI or other information that could be compromised due to theft or demands to view information (including encrypted information) during border security checks.

1.4 Reporting of Lost or Stolen Mobile Devices or Removable Media

1.4.1 Report lost or stolen items to Manager and ITS (see ITS Infonet forms).
1.4.2 ITS reports the lost or stolen item to Director, Enterprise Risk Management.
1.4.3 If the device contained (or might have contained) Personal Health Information (PHI) or other SHR information that could be classified as confidential, ITS shall report the lost or stolen item to the SHR Privacy Officer.

2. REFERENCES

Best Practices. Mobile Device Security. May 27, 2009. Office of the Information & Privacy Commissioner of Saskatchewan Website: http://www.oipc.sk.ca
SHR User Account Policy
SHR's Password Policy
SHR's Information Classification, Labelling, and Handling policy
SHR's Email Acceptable Use policy
SHR's Emailing Personal Health Information policy

Additional information is available on the ITS InfoNet Site – see "Frequently Asked Questions"

Appendix A – USB Flash Drive Security Guidelines

USB flash drives have gained popularity due to their huge data storage capacity, simplicity of use and portability. The problem with these devices, however, is their size and the potential for misplacement, loss or theft. If the USB flash drive goes missing it is more than likely that data has also gone missing.

The use of USB flash drives might simplify life but unless adequate security measures are taken, the data and the Saskatoon Health Region will be left vulnerable to data loss and the possibility of legal action. Fortunately, there are some easy steps that can ensure the safety of USB flash drives.

The following steps are intended to help ensure proper use of USB flash drives:

- □ Know the classification of data that you are storing on the USB flash drive.
- □ If you are placing Confidential data on the USB flash drive:
  - □ Ensure that the data is encrypted as soon as it is stored on the device.
  - □ Ensure that the text 'Confidential' appears on the media's label.
- □ If you are consistently using a USB flash drive for internal or confidential SHR data, you **must** utilize a USB flash drive that automatically encrypts the data as soon as it is saved and does not offer the user an option to do otherwise. For currently recommended SHR standards for this type of product, please see Forms > Computer Equipment Requisitions on the ITS InfoNet.
- □ Make sure all USB flash drives are password protected in order to protect against unauthorized access.
  - □ Create and use a complex password that meets the requirements of SHR's Password Policy. If this is not possible, the password that is chosen should meet as many of the policy's requirements as possible.
- □ Some USB flash drives come with biometric finger print identification software that helps recognize the legitimate user. The software scans finger prints, authenticates the user and only then allows him/her to access the data. This can streamline the need for passwords.
- □ Once you are done with the data remove it from the USB flash drive. Do not carry extra or old data files on the USB flash drive.
- □ Check the USB flash drive on a regular basis to ensure files are encrypted and that no unnecessary files have been accidentally left behind.
- □ Don't share your USB flash drive with someone else unless they have a valid business or clinical need to see the data contained on it or you have removed all the data from it.
- □ Place the USB flash drive on a chain and attach it to your building access key or card. This will help keep track of the USB flash drive and minimize misplacements or loss.
- □ Always put the USB flash drive away when not in use (e.g. in your pocket, purse, laptop case, etc.)
- □ When back at your office, store the USB flash drive in a locked drawer or cabinet. Never leave it on your desk or in line of sight.
- □ If a USB flash drive is misplaced, lost or stolen, notify your direct supervisor. Your supervisor should report the incident to IT Security or, as appropriate, the SHR Privacy & Compliance group.

What have you been able to √ off?

Taking these steps will ensure safe usage of a USB flash drive.