Use of Portable Electronic Storage Devices

Reviewed Date		**Number**	*TQ0107*
Revised Date	Superseded by Directive of the Medical Officer of Health February 19, 2010 August 25, 2010	**Approved Date**	*November 30, 2005*

Introduction

Purpose

DVD /CD burners and Pen Drives can be used to transfer data quickly and easily. They are particularly convenient for carrying PowerPoint presentations to other organizations that already have a computer hooked up for multiple presentations and for transferring working documents/reports for further work to another computer.

Legislative Authority

Policy Definitions and Interpretation

Risks:

Use of these electronic storage media can expose the agency to vulnerabilities including:

- Breach of confidentiality due to copying and transporting of confidential information including personal health information.
- Exposure of the computer network to viruses transported on these media.
- Inefficiencies including the waste of human resources and materials as a result of using these tools inappropriately.

This policy establishes the expectations and parameters for use of these tools in the conduct of health unit business in order to minimize the risks to the agency.

Definitions:

Pen drives

Also known as flash drives, jump drives or memory sticks, these storage media are affordable and provide quick, dependable data transfer. Because there is no driver software to install they can be used immediately after being plugged into a USB port on virtually any computer. These drives are virtually indestructible but may be susceptible to viruses and loss.

CD/ DVD

CD-R can be written only once but can be read by practically any other device. The disc is less tolerant to extreme temperatures and more susceptible to physical damage

CD-RW can be written on and erased 1,000 times. They are more expensive but can be reused.

All CD/ DVD devices must have appropriate software installed and CDs can be time consuming to burn.

Policy

Note: This policy was superseded by the following directive from the Medical Officer of Health February 19, 2010 and August 25, 2010.

General:
The copying and transporting of personal information including personal health information on unencrypted devices is prohibited.

Staff are prohibited from connecting personal electronic storage devices to agency systems. This includes but is not limited to personal pen drives, flash drives, portable hard drives and PDAs.

Staff can continue to use agency-issued cell phones, blackberries and agency camera equipment/memory cards provided they are not used to download or transport personal or personal health information.

Pen drives and other mobile storage devices used by third parties (people from outside organizations, contractors) should not be connected to agency systems. Where alternative processes are not feasible, controls will be put in place to reduce the risk of unauthorized copying of agency information to these devices and the potential risks to the security of our systems. See below for parameters.

Where possible, only encrypted mobile devices should be used to copy and transport agency information. Where the use of an encrypted device is not feasible, controls will be put in place to reduce the risk of copying personal information by error or omission. See below for parameters.

Pen drives:

The agency has a supply of encrypted pen drives for use by all staff to copy and transport agency information.

Where a third party (i.e. a presenter) requests permission to use an unencrypted pen drive on our agency equipment other alternatives will be investigated including:

- ensure the information being transported is not personal or personal health information
- emailing the presentation
- downloading the presentation to the individual's computer and hooking up to our DPM
- providing the individual with a guest account to our wireless network to enable them to access their network remotely through the internet
- if these alternatives are not feasible, use of a pen drive with the presentation on our equipment would be a last option. The laptop used to read the pen drive should not be connected to the network at the time of the mobile device being used and should have our most up to date virus protection.

DVDs/CDs:

The copying and transporting of unencrypted personal or personal health information onto CDs and DVDs is prohibited.

Playing commercially purchased CDs and DVDs on our equipment is approved.

Burning of **non-personal** information to a CD or DVD is permitted when required for program purposes. The responsibility for burning information to a CD or DVD will be restricted to specific administrative support staff within each service. The individuals responsible for burning CDs and DVDs will also be responsible for logging and tracking the copying of information and the distribution of the media. Service management will be responsible for identifying the designated support staff for their service area and for ensuring the appropriate tracking systems are in place.

Receiving and playing a CD or DVD from another organization should carry several cautions:

- ensure the information being transported is not personal or personal health information;
- for presentations if there is a way for a presenter to bring these into the organization (on their own laptop hooked up to our DPM or emailing them to the event coordinator in advance) that would be preferred but a burned CD or DVD would be acceptable in the absence of the other options.
- ensure that the unit that the DVD or CD is being played on is regularly connected to the network so that the virus checker is up to date.

Hard drives, flash drives etc.

Use of these devices is prohibited unless approved as an exception by the MOH.

Procedures

Pen Drive Access – General

1. Encrypted Pen Drives will be issued for general use to PAs in all outer offices and ACs in the Barrie Office:
2. Designated administrative staff will ensure that individuals sign out the pen drives acknowledging responsibility for the protection and proper use of the pen drive using standardized sign out sheets (Schedule 2)
3. The designated administrative staff will be responsible for monitoring the inventory once a week.
4. Pen drives available for general use will only be used to copy and transport information - not as a holding drive. After use of the pen drive, the information should be copied back to the server and removed from the pen drive.
5. Employees will consult with their contacts at external agencies to gain authorization from that agency before attempting to connect to their systems using a pen drive. This could be seen as a security breach to their system.

CD Burners – Access

- Requests for burning of material to a CD will be made through designated service administrative personnel with 48 hours in advance.

- Individuals will be responsible for ensuring that the disk has been copied appropriately and that the disk can be read in the computer they are using.
- Individuals are responsible for securing and disposing of disks in an appropriate manner.

Related Forms

TQ0107 - Pen Drives - User Requirements

Related Policies

Final Approval Signature: _____
Review/Revision History:
September 2010 Policy re-numbered, previous number C4.100