Portable Electronic Storage Devices

Scope: Eastern Health
Executive Sponsor: Chief Finance Officer
Policy Status: Revised
Last Review Date: 02-02-2009

Policy Number: 347
Approving Body: EH Corporate Quality Council
Policy Developed: 01-06-2007
Next Review Date: 07-02-2012

Purpose:

The purpose of this policy is to minimise Eastern Health's exposure through loss, misuse or unauthorised access to sensitive information contained on portable electronic storage devices.

Details:

Rationale

Eastern Health provides portable personal computers and blackberry communication devices to staff whose duties require mobility. Information stored on these devices, as well as other portable storage media such as CD-ROM, Floppy Disc, USB Memory Sticks, Portable Hard Drives etc, is vulnerable to loss, theft or unauthorised access.

Policy

Staff are bound by a strict code of confidentiality which is underpinned by Eastern Health's Privacy policy and encapsulates the requirements of the Health Records Act (2001) and the Information Privacy Act (2001). In order to reduce the potential for exposure to Eastern Health from accidental or intended misuse, disclosure or loss of sensitive data all staff are expected to abide by the following guidelines.

Guidelines

General

Staff are responsible for the security of portable devices and any information contained on them at all times.

Where possible all files stored on electronic storage media or portable storage devices should have appropriate password protection or encryption enabled.

Devices must not be left unattended in public places or in unattended motor vehicles.

Information relating to patients, hospital personnel or commercially sensitive information (including financial information) must not be stored on, or copied to portable storage or media devices without written approval of the relevant General Manager. This includes the C:\ drive of portable personal computers. Eastern Health's ICT Department provides secure storage for corporate, personal and patient information on its network servers and where appropriate can provide a secure, remote (VPN) access to such information if business needs exist.
Copying of hospital information onto privately owned computers or storage devices is not permitted.

**Portable Storage Media**

Copying of patient or staff personal information to portable storage media is not permitted.

Where other potentially sensitive information is required to be stored on portable devices, all files should be password protected and where possible, encrypted to protect against unauthorised access.

**Laptop Computers**

All personal computers must have appropriate access protection e.g. password protection must be enabled at logon to operate the computer.

Personnel requiring remote access (i.e. work from home) to official information stored on network servers may be provided with VPN access.

Passwords must not be written down and stored with the computer.

Patient or staff personal information should only be stored on a secure personal or departmental folder on the hospital's primary network server. If a requirement exists to copy patient or staff personal information onto portable storage media written approval from the relevant General Manager must be sought.

Where other potentially sensitive information is required to be stored on personal computers, all files should be password protected and where possible, encrypted to protect against unauthorised access.

Loss or suspected theft must be reported immediately to the ICT Department.

**Blackberry, Mobile and PDA Communications Devices**

The Security PIN Code feature must be activated to require a PIN to operate the device.

Loss or suspected theft must be reported immediately to ICT Department who will immediately delete the email account where applicable.

Eastern Health will secure its information in accordance with their importance and risk of loss to the organisation. An information risk assessment process will determine the level of security and service required for the information.

In the protection and security of mobile devices such as Blackberries, Eastern Health ICT enforces protection on organisation data through the use of security configuration settings provided by a centralized BlackBerry Enterprise Server. The user changes enabled are:

BlackBerry Device Security Settings:

1. **Passwords are required**
   a. Minimum password length is six (6) characters
   b. Users cannot disable password requirement

2. **Timeout**
   a. Maximum inactivity timeout is 10 minutes before you are required to re-enter password.
   b. You will also be required to re-enter your password before you unlock the device.

3. **Attempts**
   a. Maximum password entry attempts is ten (10)
   b. IMPORTANT: Device will lockout and wipe all local data from the device!!! After ten (10) attempts with the wrong password. Please call the Eastern Health local IT helpdesk BEFORE attempting ten (10) logins if you forget your Blackberry password.
Policy History

Created June 2007
Revised February 2009

Dissemination/Education Strategy

To be made available to all staff via the Eastern Health Objectify system

Related Policies

Privacy of employee records
Access to computer systems
PC Usage Policy - User Responsibilities
Use and disclosure of information
Privacy

Policy Upload:

Portable electronic storage devices Checklist.doc