16.0 Information Management

16.4 Organization and Security

16.4.2 Protection

16.4.2.5 Mobile Computing

1.0 Purpose

The use of mobile devices such as laptops, Blackberry™ devices or Personal Digital Assistants to access, store, or process information increases the risk of information compromise. Portable storage devices are typically small, portable, used in uncontrolled public environments and are easily lost, stolen or damaged.

The purpose of this policy is to protect information stored on ***mobile devices*** from loss, unauthorized access and unauthorized disclosure.

2.0 Scope

This policy applies equally to all individuals associated with the VIHA (collectively defined as "Individuals") including:

- Employees of the VIHA, and those involved with its affiliated programs and agencies, including students;
- CEO, executives, management, and supervisory employees;
- Members of the VIHA Board of Directors;
- Volunteers of the VIHA;
- Staff on contract;
- Physicians with privileges at any VIHA site;
- Medical staff including physicians on contract, residents, and clinical trainees;

- University faculty and support staff who work at VIHA facilities; and
- Any authorized user of VIHA information systems or information in the custody and control of VIHA.

3.0 Policy

Individuals using mobile devices must:

- Comply with all applicable policies, procedures and laws;
- Ensure that use of mobile devices is managed and controlled to mitigate the inherent *risks* of portable storage devices;
- Ensure that information and information technology assets in their custody or control are protected;
- Protect Userids and user credentials to reduce the risk of unauthorized access to information and information technology assets. In particular, users must protect against visual eavesdropping of passwords, PINs and other credentials, especially when in public places;
- Limit the storage of personal information on mobile devices to only that which is absolutely necessary to conduct VIHA business; and
- Be familiar with the operation of protection technologies and security incident reporting procedures.

All individuals have a responsibility to report violations of this policy without fear of reprisal. Individuals deemed responsible for violations of this policy may be subject to penalty or sanction up to and including termination of employment, cancellation of contract or services, termination of the relationship with VIHA, withdrawal of privileges and/or legal action.

4.0 Standards

The following protection technologies and controls must be implemented on mobile devices used to conduct VIHA business:

- Network access to portable storage devices from non-VIHA networks must be blocked by implementation of firewall or filtering technologies to protect against attack (e.g., to prevent network attacks against the mobile device).
- Mobile devices must be protected against *mobile* and *malicious code* using antivirus software enabled in real-time protection mode and updated daily.
- Portable storage devices must be locked and/or secured when unattended to prevent unauthorized use or theft (e.g., use device locks, cable locks, physical container locks, PINs or screensaver locks).
- Encryption of sensitive information stored on mobile devices to prevent information loss resulting from the theft of the device;
- Encryption of sensitive information transmitted via public networks;

- Transmission or storage of sensitive information must utilize an industry standard encryption algorithm (SSL, AES, 3DES etc) with a minimum key length of 128 bits;
- Access control permissions must be applied to prevent unauthorised access to information by system users, particularly for multi-user mobile systems;
- Regularly maintained data backups of information stored on mobile devices using VIHA backup facilities to protect against information loss;
- Mobile devices must not be used to store the only copy of a VIHA record;
- Physical security of the device must be maintained at all times to protect against asset and information loss; and
- User authentication to the portable storage device and user authentication for remote access from the device must be implemented.

The following risks inherent with the use of mobile devices must be assessed prior to using mobile devices to store sensitive information or conduct VIHA business:

- Data classification and sensitivity;
- Unauthorized access and disclosure;
- Public trust;
- Physical theft;
- Data interception;
- Credential theft;
- Unauthorized device use;
- Device destruction;
- Information destruction;
- Covert key logging or password harvester programs; and,
- Malicious and mobile code.

5.0 Definitions

Control - of Information (contained in a record) means the power or authority to manage the record throughout its life cycle, including restricting, regulating and administering its use or disclosure.
The following are some of the factors indicating that a public body has control of a record:

- The record was created by a staff member, an officer, or a member of the public body in the course of his or her duties;
- The record was created by an outside consultant for the public body;
- The record is specified in a contract as being under the control of a public body;
- The content of the record relates to the public body's mandate and functions;
- The public body has the authority to regulate the record's use and disposition;
- The public body has relied upon the record to a substantial extent;
- The record is closely integrated with other records held by the public body; or,

- The contract permits the public body to inspect, review, possess or copy records produced, received or acquired by the contractor as a result of the contract [1].

Custody - of Information (contained of a record) means having physical possession of a record, even though the public body does not necessarily have responsibility for the record. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing, and providing security.

Information: Any operational data or information gathered, processed transmitted or presented using a computer as defined as Information. This includes confidential personal health information and business related information.

Information Systems: Any electronic device or equipment used to support the electronic storage, transfer, or access of information.

Mobile Devices: Laptops, Tablets, Personal Digital Assistants (PDAs), Blackberry ™, Smart Phones, external hard drives, USB storage devices and any other devices that provide mobile data processing and data storage capabilities.

Sensitive Information: Any information that would not be considered public such as business, confidential or personal health information.

6.0 Additional References:

1. VIHA Policy 16.4.2.1 Security of Electronic Information
2. VIHA Policy 16.4.2.2 Security of Health Records
3. VIHA Policy 16.4.2.3 Acceptable Use
4. VIHA Policy 16.4.2.4 Remote Access
5. VIHA Policy 1.5.1 Confidential Information – Privacy Rights of Personal Information
6. Freedom of Information & Protection of Privacy Act. R.S.B.C. 1996, c. 165