	POLICY Number: 7311-25-000 Title: IT SECURITY
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Information Technology Services Cross Index: Date Approved: April 4, 2011 Date Revised: June 4, 2014 Date Effective: June 25, 2014 Date Reaffirmed: Scope: SHR & Affiliates

Overview

In today's age of information sharing and availability, information is accessible to regional, provincial and world-wide audiences. Building health information systems that are widely distributed presents an important need to ensure privacy of personal health information. Through IT security policies, structured processes are identified and a set of protection levels are established. This policy applies to any individual, service or entity granted access to clinical or business applications, information not in the public/unrestricted realm, or Personal Health Information (PHI).

DEFINITIONS

Information Technology (IT) Security means the protection of data against accidental or malicious disclosure, modification, or destruction through implementing controls that protect the confidentiality, integrity, and availability of information and information systems.

ISO 17799 (also referred to as ISO 27002) means a comprehensive set of internationally reviewed and recognized controls endorsed by the International Organization for Standardization compromising best practices in the area of information security management. Health care departments at both the provincial and SHR levels are modeling their IT policy after the recommendations contained within ISO 17799.

Saskatoon Health Region (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.

1. PURPOSE

The purpose of this policy is to establish Saskatoon Health Region's position and requirements regarding IT security. This framework creates the foundation and structure within which a comprehensive set of IT Security safeguards can be developed.

2. PRINCIPLES

IT Security principles address both the technical and non-technical issues, combined to satisfy legislative and business requirements. SHR Users are considered at the centre of the security principles.

The following principles identify the requirements for IT security:

2.1 **Authentication:** Proving identity. Access to information requires authentication via a password or some combination of tokens, biometrics, and passwords. In some cases multiple factor authentication may be required. Typically, multiple factor authentication is achieved by interrogating more than one aspect of a user (e.g. who they are, what they have, what they know, and/or where they are) rather than relying on the answer to only one of these types of questions.

2.2 **Authorization:** Granting approval. Authorization to access information within an application can be based on individual or role-based access controls.

2.3 **Encryption:** Applying a mathematical function that transforms every character in the file into some other character. Encryption renders the file unreadable. This means no one can read the file until it is decrypted. Only the authorized users can decrypt the file.

2.4 **Integrity:** Ensuring information is protected from unauthorized alteration or destruction, whether accidental or deliberate.

2.5 **Accountability:** Ensuring the ability to track and monitor activities associated with the access and use of systems, interactive and automated, messaging and online.

2.6 **Non-Repudiation:** Ensuring the ability to associate, within a legal framework, access, activities and transactions to a specific individual in a manner that can not be disputed.

2.7 **Availability:** Ensuring health information stays operational and accessible to system users. Generally this is discussed in terms of uptime. As uptime requirements increase so do the steps required to ensure:

- *fail-over* (transferring of information processing or communication to secondary IT infrastructure when primary IT infrastructure fails, ideally in a manner that is transparent to the end user),
- *redundancy* (having backup or duplicate IT infrastructure available in case primary hardware fails),
- *data backup* (saving a secondary copy of data so that information is not lost due to IT hardware failure) and
- *fault tolerance* (architecting IT services to prevent or compensate for single points of failure)

2.8 **Risk Management:** Protecting information based on its value (classification or criticality) and the risk of loss or compromise.

3. POLICY

3.1 SHR shall maintain a comprehensive set of IT security policies and procedures to monitor use and access of SHR information assets.

3.2 All IT security policies shall use ISO 17799 as a benchmark.

3.3 The scope of the IT security policies include, but is not limited to:

3.3.1 Individuals, services and or entities that are:

- SHR employees;
- Physicians, residents, and other health care professionals;
- Students;
- Contractors;
- Consultants;
- External auditors;
- Vendors;
- Other governmental agencies;
- Other third party accesses.

3.3.2 Information resources specific to the electronic domain, which include:

- Applications/software/databases;
- Storage media/removable storage;
- Personal Computers/Laptops/tablets/PDA's/Wireless devices
- Servers/minicomputers/mainframes;
- Peripherals;
- Data Centres/service centres/any facilities that house the above defined information.

3.3.3 Components used in the processing of the information:

- Data
- Hardware
- Software
- Personnel

3.3.4 Related Environments that will have access to the information:

- Management
- Development
- Certification
- Production

3.3.5 Physical facilities and locations that will manage and contain the information:

- Call Centers
- Data Centers
- Development Facilities

3.3.6 Information Systems, through all phases of their lifecycle:

- Initiation
- Construction
- Delivery
- Usage
- Retirement

3.3.7 Information throughout its entire lifecycle:

- Collection
- Use
- Access
- Storage
- Disposal

3.4 IT Security policies shall:

- Protect, prevent, and detect malicious activities;
- Assist in the understanding of potential security exposures, and risks;
- Educate, communicate and promote security responsibilities to all stakeholders;
- Ensure compliance with legislative, privacy and contractual requirements;
- Identify consequences of security policy violations.

3.5 SHR shall put reasonable procedures in place to monitor the use and access of SHR information assets.

3.6 An impartial annual security review or audit of SHR's security practices shall be conducted by a qualified independent department, manager, or third-party organization in order to measure compliance with SHR Privacy and Security policies and IT Security Standards. SHR affiliates must receive a report of any SHR audit or review results pertaining to information, information systems, or databases that belong to them.

3.7 Due to the nature of business conducted within SHR there may be a need to perform tasks that are seen as non-compliant with SHR IT Security policy. When a valid need arises, approval from business unit management at the Director or VP level and either SHR's Director Information Technology Services or Manager IT Governance, Risk and Compliance will need to be sought, granted and documented on a case-by-case basis. When such actions may affect the integrity of the information, information systems, or databases owned by SHR affiliates, approval from the CEO/CFO of the respective affiliate site(s) must also be obtained and documented.

4. ROLES AND RESPONSIBILITIES

4.1 SHR Users

4.1.1 Comply with SHR IT security policies, standards, and safeguards.

4.2 Information Technology Services (ITS) department

4.2.1 Establish and implement policies and standards that will ensure the security of SHR computerized systems and electronic data.

4.2.2 Coordinate and conduct assessments and reviews to ensure IT Security policies are updated appropriately to correspond with technological changes.

4.3 SHR Departments & Affiliates

4.3.1 Conduct an impartial annual security review or audit of IT Security policies and ensure associated operational practices are in compliance with same.

5. POLICY MANAGEMENT

The management of IT security policy, which includes policy education, monitoring, interpretation, implementation and amendment, is the responsibility of the Director, Information Technology Services.

6. NON-COMPLIANCE/BREACH

Non-Compliance with SHR IT Security policies by SHR employees or employees of contractors providing services to SHR may lead to disciplinary action including dismissal if the breach is intentional, major or relates to Personal Health Information. Violations may also result in significant legal fines and/or imprisonment[1] for the offending individual(s).

7. REFERENCES

eHealth Saskatchewan Security Policy Framework

[1] HIPA Section 64(2)(a)