



# Brandon Regional Health Authority

## Privacy and Security Assessment 2008 .....

Our Journey

Prairie Health Information Privacy  
Day 2008

# Intro to Brandon RHA



- **Regional Referral Centre serving approximately 180,000 people**
- **2400 staff and over 100 physicians**
- **Wide range of health services that include:**
  - **Acute Care**
  - **Ambulatory Care**
  - **Long Term Care**
  - **Primary Care**
  - **Variety of Community Programs, and**
  - **more**

# Background

**In 2003 two multi-disciplinary, cross regionally represented committees were established:**

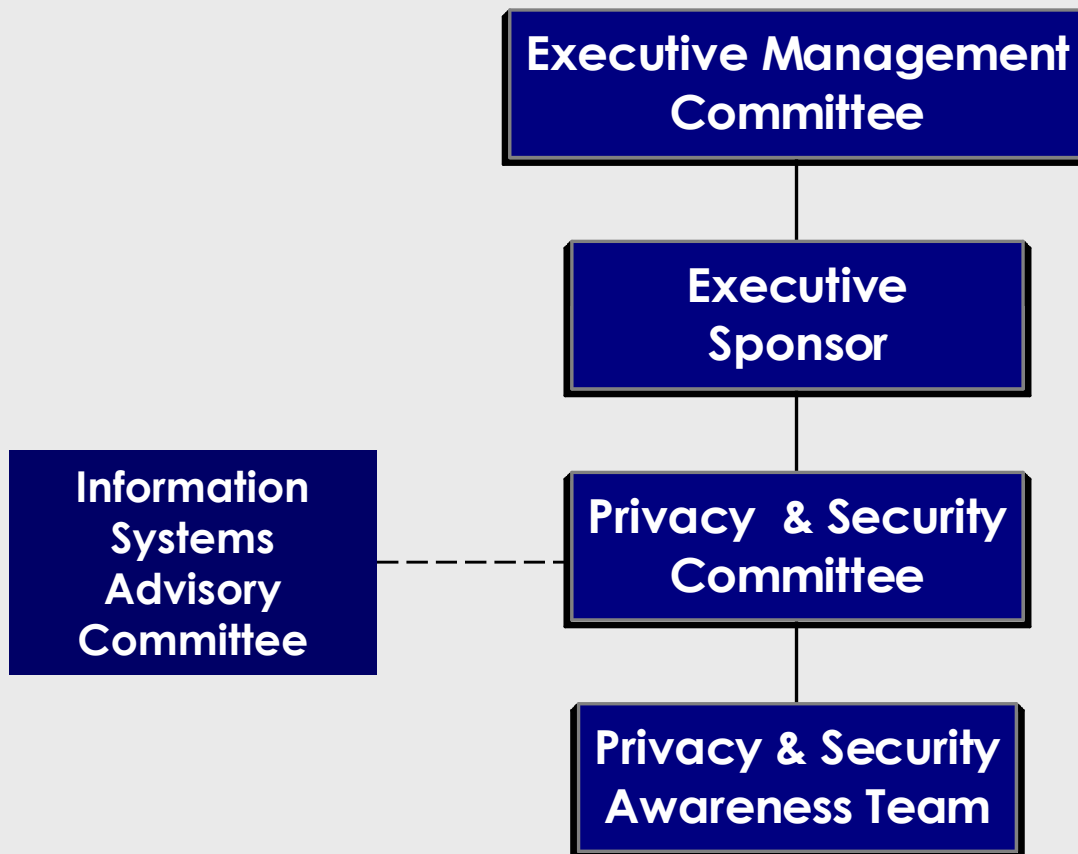
## **❖ Privacy & Security Committee**

- **Establish a secure information management environment in accordance with applicable legislation and good practice**

## **❖ Privacy & Security Awareness Team**

- **Promote educational initiatives and information sharing**

# Privacy & Security Reporting Structure



## **P & S COMMITTEE MEMBERS**

- **Privacy Officer (Chair)**
- **VP, Finance & Info Services (sponsor)**
- **Info Systems Engineer, IT**
- **Director, Health Info Services**
- **Manager, Health Info Services**
- **Director, Acute Care**
- **Secretary, Psychiatric Facilities**
- **Director, Home Care**
- **Manager, Info Services, Imaging**
- **Systems Support Coordinator, Lab**
- **Coordinator, Quality Risk**
- **Clinical Applications, EHR**
- **Manager, Human Resources**
- **Manager, Security Services**
- **Administrative Secretary,  
Mental Health Services**
- **Resident Care Manager, PCH**
- **Director, Pharmacy**

# 2004

- **Privacy & Security Committee**
  - **Conducted a “Self Assessment”**
    - **Snapshot**
  - **Developed a Strategic Plan**
    - **Progress stalled**

# 2008

- ❖ **Fall of 2007 – P & S Committee decided to conduct a more comprehensive assessment**
  - ❖ **Used as part of the requirement under PHIA 8(1) to conduct an audit of security safeguards at least every two years**
  - ❖ **All forms of confidential information (FIPPA, Mental Health Act)**
  - ❖ **Information Technology resources and infrastructure**
  - ❖ **Form a foundation for future reviews**

**Purpose: To review the information assets, information technology resources and infrastructure and the privacy and security practices within the Brandon RHA to ensure the protection all confidential information**

# Assessment Tool and Guide

- ❖ Pre-existing self assessment tool
- ❖ Developed a guide
- ❖ COACH guidelines (2004)
- ❖ Infoway Privacy & Security Requirements

**148 elements included in the assessment**

# Assessment Categories

- ⇒ **Organizational Privacy & Security Management**
- ⇒ **Personnel Security**
- ⇒ **Physical Security**
- ⇒ **Hardware Security**
- ⇒ **Communications and Network Security**
- ⇒ **Software and Database Security**
- ⇒ **Operations Security**
- ⇒ **Information Security**

# Method

## Assessment completed by:

- ❖ Privacy & Security Committee
- ❖ Information Technology Managers and the delegated Security Officer

1. Each element within the assessment categories was reviewed to determine if they exist or not (Note: P was used where we partially met the requirement)

REF	ELEMENT	YES	NO
-----	---------	-----	----

2. Where an element does not exist, or partially exists, a level of risk associated with the absence of the element is assigned

REF	ELEMENT	YES	NO	RISK RATING L - M - H
-----	---------	-----	----	--------------------------

# Risk Level

		Severity of an Occurrence			
		Catastrophic	Major	Moderate	Minor
Probability of Occurrence	Frequent	High	High	Medium	Low
	Occasional	High	High	Medium	Low
	Uncommon	High	Medium	Medium	Low
	Remote	High	Medium	Low	Low

High

Medium

Low

## Method, cont'd

### 4. The current practice for each element is described

REF	ELEMENT	YES	NO	RISK RATING L - M - H	CURRENT PRACTICE
-----	---------	-----	----	--------------------------	------------------

### 5. Opportunities for improvement were identified (Including existing elements)

REF	ELEMENT	YES	NO	RISK RATING L - M - H	CURRENT PRACTICE	OPPORTUNITIES FOR IMPROVEMENT
-----	---------	-----	----	--------------------------	------------------	----------------------------------

# Personnel Security

❖ Personnel security is a key component of developing a security-conscious environment. Protection of confidential information needs to be second nature to all personnel handling information assets

❖ Developing and maintaining security conscious behaviour begins on introduction to the RHA and continues throughout the lifespan of an individual's association through:

- ❖ Education and awareness,
- ❖ Policy and procedure
- ❖ Leadership
- ❖ Incident reporting and disciplinary process

# Personnel Security

REF	ELEMENT	YES	NO	RISK RATING L - M - H	CURRENT PRACTICE	OPPORTUNITIES FOR IMPROVEMENT
B6	Ongoing privacy & security refresher training for all employees	X			<ul style="list-style-type: none"> <li>• Privacy &amp; Security Awareness Team oversees monthly education briefs in Regional Responder as well as workshops and other initiatives</li> <li>• IT Security newsletter</li> <li>• Privacy Officer available for staff meetings</li> <li>• Designated security awareness month</li> <li>• All new staff provided with an IT orientation package (B6a)</li> <li>• IT educator available to assist with education needs</li> <li>• Pledge forms part of performance appraisals</li> <li>• IT Education and Orientation policy (B6b)</li> </ul>	<ul style="list-style-type: none"> <li>• Information available to staff on the intranet (I.e. FAQ's)</li> </ul>

**PR 22b Training Users and Raising Awareness**

**SR 16 Training Users and Raising Security Awareness**

# Communications and Network Security


- ❖ **The network is the backbone of all communications and information processing. A secure internal infrastructure that includes system surveillance and monitoring, strong authentication, and use of security technology ensures the confidentiality and integrity of data. Developing communications and network security strategies is key to ensuring data is protected from interception or unauthorized access, disclosure or modification.**

# Communications and Network Security

REF	ELEMENT	YES	NO	RISK RATING L - M - H	CURRENT PRACTICE	OPPORTUNITIES FOR IMPROVEMENT
E13	Use of industry standard encryption to secure confidential communications		X	H	<ul style="list-style-type: none"> <li>• No encryption available for email</li> <li>• Staff are directed to contact IT for assistance with securing confidential communications to external parties</li> <li>• Free third party solutions are occasionally used to Password protect communications</li> </ul>	<ul style="list-style-type: none"> <li>• Pursue funding for an email encryption system that meets MB Government/eHealth standards</li> <li>• Develop procedure for consistent process in the interim</li> <li>• Continue to educate staff re risks and safeguards for confidential communications</li> </ul>
	<div style="background-color: #000080; color: white; padding: 5px;"><b>SR 31 Encrypting PHI during transmission</b></div>					

# Information Security

 Information Security enables the protection of information assets from an information management perspective.

 Information management includes the tools and processes to enable personnel to ensure appropriate access, use, collection, disclosure, retention and destruction of information

# Information Security

REF	ELEMENT	YES	NO	RISK RATING L - M - H	CURRENT PRACTICE	OPPORTUNITIES FOR IMPROVEMENT
H9	Audit trail of all user access to personal health information	XP		H	<ul style="list-style-type: none"> <li>• Not all systems have the ability to audit. Some applications are waiting for upgrades to include audit function</li> <li>• Access to some applications has been restricted until audit functions are available</li> <li>• Internally developed systems have audit trails</li> <li>• See list of systems and audit functionality (H9)</li> </ul>	<ul style="list-style-type: none"> <li>• Continue to work with vendors to enhance current systems to meet audit requirement</li> </ul>

***PR 19 Logging Access, Modification and Disclosures***

***SR 40 Preserving the History of phi in POS systems***

***SR43 Minimum Content of Audit Logs***





# Physical Security

- **18 elements**
- **Walk through all facilities**
- **Staff interviews**
- **Reviewed information assets in each area**
- **Reviewed information technology resources in each area**
- **Each program will be provided with a summary of our findings – strengths and risks**

# Results

- ❖ **Close to 200 opportunities to improve were identified**
- ❖ **All have been grouped into the following 5 categories**
  - **Policy & Procedure**
  - **Personnel**
  - **Technology**
  - **Physical & Process Change**
  - **Education**

# Action Plan

-  **Draft Action Plan has been created**
-  **Only Medium and High Risk elements**
-  **Grouped into the 5 groupings**
-  **Education action items will be addressed through the Privacy & Security Awareness Team**

## **Where we are at today**

- **Assessment is complete**
- **Executive summary is complete**
- **Draft Action Plan has been developed**

# The Road Ahead

- **Executive Summary will be submitted to Executive Management Committee**
- **Action Plan will be finalized and work initiated**
- **Summary reports will be provided to all programs**
- **Review in 3 years**

# Challenges

- 1. System functionality restrictions (older systems)**
- 2. Financial Resources**
  - System upgrades
  - Architecture upgrades
  - Purchase of new technology
- 3. Human Resources**
  - Monitoring user activity
  - Policy & Procedure development

# **Lessons Learned on the Road**

**Our Journey continues.....**

**As we look at the long road ahead,**

**we need to stop frequently and  
remind ourselves .....**

**We've covered more miles than  
we think!!**