OFFICE OF THE
AUDITOR GENERAL
MANITOBA

Website Version

Department of Health, Healthy Living and Seniors

WRHA’S Management of Risks Associated with End-user Devices

July 2015

Our vision

The Office of the Auditor General is an accessible, transparent and independent audit office, serving the Manitoba Legislature with the highest standard of professional excellence.

Our values

- Respect
- Honesty
- Integrity
- Openness

Our priorities

- Strengthen the management systems and practices of government organizations
- Provide Members of the Legislative Assembly with relevant information
- Manage our internal business effectively

Our critical success factors

- Independence from government
- Reliable audit opinions and conclusions
- Relevance of audit work performed
- Knowledge, skills and abilities of our staff

OFFICE OF THE
AUDITOR GENERAL
MANITOBA

July 2015

The Honourable Daryl Reid
Speaker of the House
Room 244, Legislative Building
450 Broadway Avenue
Winnipeg, Manitoba R3C 0V8

Dear Sir:

It is an honour to present my report titled: *WRHA's Management of Risks Associated with End-user Devices*, to be laid before Members of the Legislative Assembly in accordance with the provisions of Sections 14(4) and 28 of *The Auditor General Act.*

Respectfully submitted,

Original document signed by:
Norm Ricard

Norm Ricard, CPA, CA
Auditor General

Table of contents

Auditor General's Comments

The Manitoba healthcare industry is increasingly relying on electronic records and automated processes. As end-user devices become more and more powerful, their proliferation within the healthcare system is understandable. But this proliferation increases the risk that healthcare information could fall into the wrong hands.

Manitobans expect that their personal health information will be well-protected. This is why the Province implemented the *Personal Health Information Act* (PHIA). Even though healthcare organizations must comply with the Act, compliance in itself does not ensure strong cybersecurity. The many recent information security breaches within the North American healthcare industry reinforces the need for strong cybersecurity controls.

Healthcare professionals need efficient and timely access to personal health information. But, healthcare organizations need to strike a proper balance between providing ready access to this information and protecting it. This is best achieved through sound risk management practices.

In this audit we found that the Winnipeg Regional Health Authority (WRHA) could not keep up with the growth in demand, nor properly control the use of end-user devices. As a result, the WRHA was unnecessarily vulnerable to personal health information falling into the wrong hands.

Given the ubiquitous nature of end-user devices, these deficiencies may also be present in other Manitoba Government organizations. I encourage all organizations to consider the findings and recommendations outlined in this report.

I would like to thank officials at the WRHA, eHealth Manitoba, and the Department of Health, Healthy Living and Seniors for their cooperation and assistance during this audit.

Original document signed by:
Norm Ricard

Norm Ricard, CPA, CA
Auditor General

Winnipeg, Manitoba
July 2015

Main points

Cybersecurity risks related to end-user devices

The mobility and power of end-user devices create operating efficiencies while transforming business processes. Their proliferation within the healthcare industry is understandable given the need of healthcare professionals to access critical information quickly. However, there is a risk that health organizations, in their desire to meet the demands of healthcare professionals for such technology, may inadvertently compromise the cybersecurity over sensitive and confidential information and systems accessed by these end-user devices.

End-user devices are defined as laptops, desktops, tablets, smartphones, and USB Flash Drives.

What we examined and found

We wanted to know how vulnerable the Winnipeg Regional Health Authority (WRHA) was to confidential personal health information falling into the wrong hands. As such, we looked at whether the WRHA properly managed the risks associated with personal health information being stored on, and accessed by, end-user devices. We focused our efforts on assessing the adequacy of management policies and practices and not on whether they were operating as intended.

We concluded that the WRHA was not properly managing the risks associated with personal health information stored on, and accessed by, end-user devices. As a consequence, there were significant cybersecurity control weaknesses. These weaknesses resulted in the WRHA being unnecessarily vulnerable to personal health information falling into the wrong hands.

Throughout our audit we observed that the WRHA was focused on ensuring compliance with the *Personal Health Information Act* (PHIA). While PHIA does include some security requirements, we believe that implementing a cybersecurity program based on sound risk management would invariably result in the WRHA accomplishing their goal of complying with PHIA security requirements. Focusing first on a control framework is important because compliance with PHIA does not ensure strong cybersecurity.

Our key findings are:

WRHA not aware of all significant cybersecurity risks related to the use of end-user devices

The WRHA has not identified and assessed the risks associated with end-user devices. As such they cannot be assured that risks are properly mitigated.

Many gaps in the cybersecurity controls over end-user devices

Risk assessments help determine and support the proper level of controls required, but there is nonetheless a minimum level of control rigour that should be in place to protect end-user devices.

We found that while WRHA did have some cybersecurity controls in place, there were insufficient cybersecurity controls over:

- the remote access to WRHA networks, systems, emails, contacts and calendars.
- the use of unmanaged USB Flash Drives.
- laptops and desktops.

Several factors led to limited attention to risks and controls

Factors that we believe led to WRHA’s limited attention to cybersecurity risks and controls are:

- **No strategy to manage end-user devices** – As the information and communication technology (ICT) service provider for the WRHA, eHealth is responsible for WRHA’s information technology strategic planning. But eHealth does not have a plan for how it will provide ICT services to the WRHA. More specifically, neither eHealth nor the WRHA have developed plans for how to manage the proliferation and use of end-user devices within the WRHA. The growing demand by healthcare professionals within the WRHA to access information and systems through mobile devices has resulted in eHealth implementing a Bring-Your-Own-Device program without first putting in place the necessary strategies, risk assessments and cybersecurity controls.

- **Information classification scheme not in place** – The WRHA has defaulted to one level of classification – confidential. Some instructions are included in various policies on how to handle personal health information but not for other types of confidential information. We believe the more structured approach envisioned by the WRHA *IT Security* policy is needed.

- **Security safeguards not audited** – Periodically assessing the adequacy and proper functioning of controls is essential in maintaining a strong information technology control environment. The WRHA is not ensuring that this is being done for end-user device cybersecurity controls. Such audits may have identified and addressed many of the cybersecurity control deficiencies we found in this audit.

- **Awareness training programs not sufficiently developed** – We found that the privacy and information security awareness training courses are not based on documented risk assessments, are not tailored for types of attendees based on the risk associated with job functionality (e.g. health care provider, privileged system or database administrators), and do not communicate incident handling procedures. Additionally, attendance to the training sessions has been poor, training content is missing important elements, and additional techniques are not used to promote information security awareness.

The report includes 12 recommendations.

Overall response from officials

The Department of Health, Healthy Living and Seniors (Health), the Winnipeg Regional Health Authority (WRHA) and Manitoba eHealth welcome the Report of the Office of the Auditor General (OAG) on the WRHA's Management of Risks Associated with End-user Devices, and agree with its findings. Health, WRHA and Manitoba eHealth place a high priority on the protection of information, and we believe that this audit will assist us in our ongoing efforts to achieve high standards in the protection of health information and information technology assets.

All of the OAG's Recommendations contained in its Report either are in various stages of implementation or are awaiting the completion of risk assessments that are a precondition to implementation, as detailed in our responses. We will work collaboratively with all regions (Regional Health Authorities, CancerCare Manitoba and Diagnostic Services Manitoba) to share the improvements in policies and practices resulting from these Recommendations.

Background

Why did we conduct this audit?

In September 2014, a laptop was stolen from the Buhler Centre at the University of Manitoba Faculty of Medicine at the Winnipeg Health Sciences Centre (HSC). The WRHA's investigation determined that it was a doctor's personal laptop[1]. It contained over 300 patient records involving consultations at the HSC's hepatology clinic over an 18 month period. As a result of this theft, the WRHA notified all affected parties of this potential privacy breach. This potential privacy breach highlights the risk of unauthorized access to personal health information when it resides on end-user devices.

In recent years, there have been significant technological advances in mobile computing. Employee expectations for accessing information assets, including systems and data, now extend well beyond traditional enterprise infrastructure. Sensitive corporate systems and data can now be accessed by, and stored on, end-user devices such as laptops, tablets, smartphones, and USB Flash Drives. These devices, while increasing productivity, are attractive targets for attackers – a risk that must be effectively managed.

Furthermore, the impact of security breaches may extend to effective service delivery. The Department of Health, Healthy Living and Seniors' (the Department) *Privacy Toolkit for Health Professionals* includes the results of a recent survey by *Fair Warning*, which suggests that Canadians would change their behavior in seeking health care if they perceive a risk to their privacy[2]:

- 61.9% reported that if there were serious or repeated breaches of patients' personal information at a hospital where they had treatment, it would reduce their confidence in the quality of healthcare offered by the hospital.
- 31.3% said they would postpone seeking care for a sensitive medical condition due to privacy concerns.
- 43.2% of the participants stated that they would withhold information from their health care providers based on privacy concerns.
- 50.6% said they would choose to be treated at a different hospital.
- 42.9% said they would seek care outside of their community due to privacy concerns.

About the Winnipeg Regional Health Authority

The WRHA provides health care to approximately 700,000 people living in Winnipeg, Manitoba (and some surrounding Rural Municipalities, as well as the Town of Churchill). They also provide support and specialty health care services to an additional 500,000 Manitobans. They have an annual operating budget of approximately $2.4 billion, operating or funding over 200 facilities and programs. Approximately 28,000 people work in the WRHA[3].

[1] The OAG did not audit or investigate this specific incident.

[2] A recent opinion survey conducted by *Fair Warning* – "Canada: How privacy considerations drive patient decisions and impact patient care outcomes."

[3] The information above was obtained from http://www.wrha.mb.ca/about/aboutus.php

About eHealth Manitoba

eHealth was created in 2006 by the Department as a central organization for the planning, development, coordination, oversight, and ongoing support/delivery of province-wide healthcare information and communication technology (ICT) projects (for instance eChart/Electronic Health Record).

While eHealth has a broad provincial mandate, it is also the WRHA's ICT service provider. eHealth is administratively housed as a division within the WRHA. The program is subject to all WRHA policies and processes (e.g. eHealth employees, contractors, vendors, and expenses are paid directly by the WRHA).

All other Regional Health Authorities have information technology departments that provide their ICT services. In 2010, eHealth, Diagnostic Services Manitoba, CancerCare Manitoba, all Regional Health Authorities, and the Department signed a Memorandum of Understanding "to establish the principles, terms and conditions under which the Parties will work together to provide and receive Shared Services throughout the province, and to create, enter into, and maintain Service Level Agreements among the Parties." eHealth continues to expand the ICT services it provides to these Provincial healthcare entities.

Our audit focused only on the ICT support services that eHealth provides to the WRHA.

What is Personal Health Information?

Given the sensitive nature of personal health information, the Manitoba Government implemented PHIA. This law, and its supporting regulations, provides individuals with rights to access their personal health information. It also establishes rules governing the collection, use, disclosure, retention and destruction of personal health information. It also requires individuals and trustees to protect the privacy of personal health information.

PHIA defines a trustee as: "…a health professional, health care facility, public body, or health services agency that collects or maintains personal health information." Based on this, the WRHA is a trustee of personal health information.

PHIA defines personal health information as:

> *Recorded information about an identifiable individual that relates to:*
> *(a) the individual's health, or health care history, including genetic information about the individual,*
> *(b) the provision of health care to the individual, or*
> *(c) payment for health care provided to the individual, and includes*
> *(d) the PHIN and any other identifying number, symbol or particular assigned to an individual, and*
> *(e) any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care*

WRHA policy further defines personal health information to include financial position, home conditions, domestic difficulties, and other private matters relating to the individual.

What are end-user devices?

The WRHA defines end-user devices (also known as "Portable Electronic Devices" or "PED") as laptops, cellular telephones, pagers, personal digital assistants, smartphones, and other similar devices. For the purposes of the audit, we defined end-user devices as laptops, desktops, tablets, and smartphones. In addition, we include USB Flash Drives as they can store vast amounts of data.

We also distinguish between two different categories of devices:

- *Managed* – WHRA devices configured and managed by eHealth.
- *Unmanaged* – personal devices or those owned by a third party, and not configured or managed by eHealth.

How many managed and unmanaged end-user devices access WRHA information and systems?

eHealth publishes an Approved Product Listing in order to standardize and support ICT services. This is eHealth's suite of "managed" end-user devices – it includes desktops, laptops, and USB Flash Drives. eHealth also manages smartphones and cell phones.

eHealth inventories the WRHA's managed desktops, laptops, cell phones, Corporate smartphones, and USB Flash Drives. **Figure 1** shows the total numbers of eHealth managed end-user devices within the WRHA environment.

Figure 1

End-User Device	Total
Desktops	10,622
Laptops	1,935
Cell phones	1,322
Corporate smartphones	1,135
USB Flash Drives	821

Source: eHealth (as at October 2014)

eHealth does not manage tablets or other third party/personal smartphones. The number and types of unmanaged devices that remotely access information and systems is not known.

How do end-user devices remotely access WRHA services?

Authorized WRHA staff and vendors can remotely access email, network, systems and data through many services.

Emails, calendars and contacts can be accessed using a web email access service (through any web-browser on any unmanaged device). Access can also be provided through corporate and third party/personal smartphones that connect and synchronize with the WRHA's email servers.

The WRHA network, systems, and data can be accessed through three main remote services. The first service provides user desktop functionality, including access to clinical applications, using an eHealth managed laptop. The second service provides access to multiple clinical and administrative applications (including the Electronic Medical Record, Electronic Health Record, as well as home care and hospital systems) using any managed or unmanaged device. The final service provides remote access to specified systems and applications for internal (eHealth) and external (vendors) support providers (e.g. network and system administrators), using any unmanaged device.

What are the risks associated with end-user devices?

Historically, cybersecurity controls in most organizations focused on protecting a defined perimeter and included measures such as physical security, firewalls, and intrusion detection systems. However, end-user devices can now provide individuals with access to internal systems and data from well beyond established perimeter controls. Providing this access comes with many risks. Infoway Canada's November 2013 white paper[4] highlights these end-user device risks:

> *Loss and Theft*
> End-user devices are portable in nature. If lost or stolen, unauthorized individuals could access information stored on (or accessed by) these devices as well as sensitive credential information stored on the device (e.g. passwords).
>
> *Insecure communication of information*
> Electronically transmitted information could be intercepted and accessed by unauthorized individuals.
>
> *Unauthorized application downloads*
> Users could download unauthorized applications onto their end-user devices. These applications may not have the appropriate privacy and security features, possibly resulting in malware attacks. Through such attacks, information stored on the device may be compromised and leaked.

We also believe that there is a significant risk of unauthorized remote access to systems and data. Individuals, such as vendors and system administrators, may require powerful remote access to information and systems. This privileged access to large amounts of information (e.g. large databases) can be targeted and exploited by unauthorized individuals.

[4] Infoway Canada is an independent not-for-profit corporation established and funded by the Government of Canada. One of their main purposes, while providing some funding, is to help provinces with the adoption and use of health information technologies. In November 2013, Infoway published a white paper "Mobile Computing in Clinical Settings – Using mobile devices to obtain seamless extension of the health enterprise's digital ecosystem".

Audit approach

We wanted to know how vulnerable the WRHA was to confidential personal health information falling to the wrong hands. As such we looked at whether the WRHA properly manages the risks associated with personal health information being stored on, and accessed by, end-user devices. We focused our efforts on assessing the adequacy of management practices and not on whether stated practices were operating as intended.

Our audit criteria are based on *Control Objectives for Information Technology (COBIT)* and other Information Systems Audit and Control Association (ISACA) audit programs. Management reviewed and acknowledged the suitability of our criteria.

The audit examined practices in place as of September 30, 2014. Our examination was substantially conducted between October and December 2014.

Our examination was performed in accordance with the value-for-money auditing standards established by the Chartered Professional Accountants of Canada (formerly Canadian Institute of Chartered Accountants) and accordingly included such tests and other procedures we considered necessary.

Findings and recommendations

We concluded that the WRHA was not properly managing the risks associated with personal health information stored on and accessed by end-user devices. And that as a consequence, there were significant cybersecurity control weaknesses. These weaknesses resulted in the WRHA being unnecessarily vulnerable to personal health information falling into the wrong hands.

We found that:
1. The WRHA was not aware of all significant end-user device cybersecurity risks.
2. There were many gaps in the cybersecurity controls over end-user devices.
3. Several factors led to the WRHA’s limited attention to end-user device cybersecurity risks and controls.

1. WRHA not aware of all significant end-user device cybersecurity risks

As eHealth provides all ICT services to the WRHA, it is important that they identify, manage and communicate all ICT risks within the WRHA environment.

We found that eHealth had not identified and assessed the ICT risks associated with end-user devices (e.g. loss and theft, unauthorized remote access to systems and data, unavailability of data). Officials from eHealth advised that some Threat and Risk Assessments were conducted on provincial systems and WRHA operational components (e.g. wireless network), but also indicated that their assessments were not specific to end-user devices (e.g. laptops, desktops, USB Flash Drives, smartphones, remote access).

Without risk assessments, senior management cannot be assured that proper cybersecurity controls are in place to manage or reduce the risks associated with personal health information residing on or accessed by end-user devices, nor can they be properly informed of related risk exposures.

Recommendation 1: We recommend that eHealth identify and assess the risks associated with end-user devices used within the WRHA environment.

Recommendation 2: Upon completion of risk assessments associated with end-user devices, we recommend that eHealth communicate the results of the risk assessments to the WRHA Chief Executive Officer (CEO) and that the CEO document the acceptance of residual risks.

2. Many gaps in the cybersecurity controls over end-user devices

Sensitive data breaches are common in large and complex organizations, including healthcare. To reduce data loss and theft, organizations must implement risk-based cybersecurity controls to protect data in motion (external to and across the network), data at rest (databases and systems), and data at the end point (laptops, desktops, smartphones, tablets, and USB Flash Drives). Many organizations implement cybersecurity controls to protect their internal systems (e.g. firewalls), yet their end-points (e.g. end-user devices) can often be poorly controlled.

Risk assessments help determine and support the proper level of controls required, but there is nonetheless a minimum level of control rigour that should be in place to protect end-user devices. We found that while the WRHA did have some cybersecurity controls in place, there were significant gaps which increased their vulnerability to information falling into the wrong hands. We provided the CEO of the WRHA with our detailed findings in a separate management letter. A summary of our concerns follows.

Privacy and security policy requirements not followed

The WRHA developed policies to help ensure that specific PHIA requirements are met and that information security risks are addressed. We reviewed those that are pertinent to personal health information being stored on or accessed by end-user devices (approval date in brackets). These include:

- Information Technology Security (dated June 2011)
- Computer/Internet Usage (June 2011)
- Use of Portable Electronic Devices and Personal Computers (June 2011)
- Confidentiality of Personal Health Information (April 2010)
- Security and Storage of Personal Health Information (February 2008)
- Disposal of Confidential Material, Including Personal Health Information (May 2000)

Included in these policies, are the following requirements:

Encryption	End-user devices are required to be encrypted. Personal health information cannot be stored on a smartphone that is not encrypted.
Authentication	End-user devices are required to have strong authentication.
Transmitting sensitive information	Users are not to transmit sensitive information over the Internet unless appropriately secured.
Use of personally-owned devices	These devices cannot be used for transmitting, storing or viewing work related information unless configured by Manitoba eHealth with the appropriate safeguards.

As discussed below, we found that many of the WRHA’s requirements for end-user devices were not being complied with.

Insufficient cybersecurity controls over remote access to networks and systems

We found that there were reasonable controls in place for two of eHealth's three remote services that provide users with access to corporate and clinical applications. But, there were insufficient controls over the remote service which provides privileged access through unmanaged devices (there are 1481 enabled accounts with this remote access). This is of concern because system administrators use this service to access and manage critical health care systems (that house significant amounts of personal health information).

Insufficient cybersecurity controls over remote access to WRHA email, contacts and calendars

eHealth has not implemented sufficient controls over the service that allows unmanaged devices (third party/personal smartphones and tablets) to connect to WRHA email, contacts, and calendars. During our audit, eHealth implemented a requirement that a passcode be used for all devices using this service. However, common end-user device security controls, such as encryption, anti-virus, and software/application download restrictions, have not been implemented.

In addition, the password requirements for eHealth's remote web email access service (that can be accessed through any web browser on any device) do not follow eHealth's own password standard.

eHealth has primarily applied only the default settings to their Corporate smartphones. These devices do not currently have access to clinical applications, but do access WRHA corporate emails, calendars and contacts. These default settings may not be sufficient for devices that hold personal health information.

These deficiencies are of concern because personal health information is emailed within the WRHA and could reside on these end-user devices.

No cybersecurity controls over use of unmanaged USB Flash Drives

eHealth provides encrypted USB Flash Drives as an approved product. While eHealth manages 12,557 desktops and laptops for the WRHA, only 821 encrypted USB Flash Drives were purchased through eHealth since 2008. Of concern is that eHealth allows any unmanaged USB Flash Drive to connect to a managed desktop and laptop. As a result, there is a distinct possibility that users within the WRHA are using personally-owned unencrypted USB Flash Drives when handling sensitive personal health information. This highlights two significant risks:

- Unencrypted devices containing personal health information could be lost or stolen.
- Malware could be introduced to eHealth managed laptops and desktops.

Insufficient cybersecurity controls over laptops and desktops

While various controls are in place over eHealth managed laptops and desktops (e.g. passwords, anti-virus), eHealth's use and implementation of encryption may not be sufficient to protect personal health information.

eHealth has a patch management program, but the program only requires the patching of some of the third party applications on WRHA laptops and desktops. The vast majority of security breaches experienced by organizations are the result of exploited weaknesses caused by inadequate patching of third-party applications[5]. Unpatched applications could allow unauthorized access to or disclosure of personal health information.

Recommendation 3: Upon completing end-user device risk assessments, we recommend that the WRHA implement the controls needed to reduce (to an appropriate level) the risks associated with end-user devices (including the areas of concern noted in our letter to management).

3. Several factors led to limited attention to end-user device cybersecurity risks and controls

Factors that we believe contributed to the WRHA's limited attention to cybersecurity risks and controls include:

3.1 No strategy for managing end-user devices.
3.2 An information classification scheme that is limited and fragmented.
3.3 No audits of security safeguards.
3.4 Awareness programs that are not sufficiently developed.

3.1 No strategy for managing end-user devices

An information technology strategic plan describes how information technology supports an organization's business objectives. The plan usually includes opportunities, limitations, and risks that information technology faces and the resources required to support organizational business objectives.

Clinical data and systems have strategic importance in delivering healthcare. Infoway's white paper[6] notes the importance that mobile devices will likely play in accessing clinical data and systems:

> *Outside of the implementation of electronic health records (EHRs), the use of mobile devices promises to be one of the most transformational information technologies in healthcare. Clinicians want a highly useful, portable and convenient tool to use in their practice – one that will improve workflow and become a handy channel of connectivity to applications to practice medicine from anywhere at any time.*

Information technology strategic planning helps an organization keep up with users' technology demands. The consumerization, productivity benefits and relatively low cost of end-user devices may prompt many users to acquire and implement their own technology if the technology has not

[5] Cisco 2014 Annual Security Report

[6] Infoway Canada is an independent not-for-profit corporation established and funded by the Government of Canada. One of their main purposes, while providing some funding, is to help provinces with the adoption and use of health information technologies. In November 2013, Infoway published a white paper "Mobile Computing in Clinical Settings – Using mobile devices to obtain seamless extension of the health enterprise's digital ecosystem".

been provided by the organization. This creates significant risk. By failing to plan for these scenarios, an organization may not be able to implement adequate policy instruments and controls before being exposed to significant risks or experiencing a cybersecurity incident. A 2013 Infoway white paper highlights this risk:

> *Without a comprehensive roadmap, the Health Delivery Organization could experience an increased set of risks ranging from IT resourcing and support, technology capabilities and cost, data and use governance, and enterprise privacy and security of corporate and personal health information….*

The WRHA recognizes the importance of information technology in supporting their business objectives. One of their top 15 documented risks is the "Inability of information technology to support strategic directions".

eHealth has developed the Manitoba Provincial eHealth Strategy. One of eHealth's goals within the Provincial Strategy is to "Develop the capacity to deliver mobile applications". Of note, however, is that the strategy lists a "Mobility Strategy" as an unfunded initiative.

As the ICT service provider for the WRHA, eHealth is responsible for the WRHA's information technology strategic planning. But eHealth does not have a plan for how it will provide ICT services to the WRHA. More specifically, neither eHealth nor the WRHA have developed plans for how to manage the proliferation and use of end-user devices within the WRHA.

As noted earlier, eHealth allows WRHA users to synchronize and access corporate email, calendar, and contact information on unmanaged devices. eHealth stated that the number of these connections was relatively low when first put in place in 2010. At the time of our audit however, over 3,900 unmanaged devices (smartphones, tablets) had connected to this service. There are approximately 28,000 WRHA employees (granted, not all of these individuals require remote access to WRHA email), indicating that there is room for significant growth in the use of this service within the WRHA. This needs to be properly managed.

eHealth has, in effect, implemented a Bring-Your-Own-Device (BYOD) program without first putting the necessary strategies, risk assessments, and policy instruments in place. Most importantly, as noted earlier, this has resulted in significant deficiencies in the cybersecurity controls over devices connecting through this service (see Section 2), increasing the risk of unauthorized access to confidential information.

Recommendation 4: We recommend that eHealth develop a strategic plan for the delivery of ICT services to the WRHA, including plans for remote access through end-user devices.

3.2 Information classification scheme is limited and fragmented

Information classification is a critical aspect of information management. Information assets, including paper or electronic data, can vary in importance and sensitivity. To properly protect information assets, organizations must first define sensitivity categories within which they would classify all of their information assets (e.g. public, protected, and restricted). An information classification scheme would also define the controls that must be in place to protect each class of information. This helps ensure that appropriate controls and handling procedures are in place to protect the confidentiality, integrity and availability of each class of information asset. It also helps users understand the sensitivity of the information they are handling.

Without an information classification scheme, there is a risk that an organization will treat all assets in the same manner. This can result in the over-protection of public information assets (resulting in a higher cost) or the under-protection of highly sensitive information (resulting in security breaches). In addition, users may inconsistently and inappropriately handle sensitive information assets.

The Department's *Privacy Toolkit for Health Professionals* states that trustees must have physical, technical, and administrative safeguards to ensure the security of personal health information and that they must be appropriate to the sensitivity of the information. To comply with this requirement, WRHA's *IT Security* policy states that it will:

> *…classify information based on the degree of risk and impact that could reasonably be expected to result from unauthorized disclosure or compromise to confidentiality, availability or data integrity. The WRHA shall identify and categorize information according to a classification scheme. The information classification scheme shall apply to electronic information, documentation and communications.*

We expected to find more than one level of classification within such a complex healthcare environment. For example - personal health, corporate (WRHA finances and operations), and public information.

However, despite the policy, the WRHA has defaulted to only one level of classification – confidential. Their *Confidentiality* policy broadly defines confidential information as:

> *…all information not readily available to the public or which would expose the Authority to charges of breach of trust including, information regarding: patients, employees and business affairs of the Authority.*

Many of the WRHA policy instruments provide instructions on how to handle personal health information (e.g. collection, correction, disclosure, use, disposal). But the WRHA's policies do not indicate whether other types of confidential information are to be handled in the same manner. In addition because instructions are provided within various policy documents, rather than in one information classification document, it is more difficult to reference and understand expectations.

We believe the more structured approach originally envisioned by the WRHA *IT Security* policy is needed.

We did not review WRHA's policy instruments to determine if they provide sufficient direction on how to handle personal health information.

Recommendation 5: We recommend that the WRHA define and implement a structured information classification scheme that includes multiple classifications based on the sensitivity of information.

3.3 No audits of security safeguards

Periodic auditing of established safeguards is essential in maintaining a strong information technology control environment. An audit can find gaps between stated requirements (e.g. policy instruments) and actual safeguards and practices in place. Also, it can identify deficiencies in the control framework. This good practice is embedded in PHIA.

The PHIA audit requirements are:

> *A trustee shall conduct an audit of its security safeguards at least every two years.*
>
> *If an audit identifies deficiencies in the trustee's security safeguards, the trustee shall take steps to correct the deficiencies as soon as practicable.*

The Department defines security safeguards in their *Privacy Toolkit for Health Professionals*:

To ensure the security of personal health information, trustees must have:

1. *<u>Physical</u> safeguards (i.e. proximity reader ID badges, locked rooms and sections, lockable filing cabinets).*
2. *<u>Technical</u> safeguards (i.e. passwords, secure networks, encryption software, firewalls, antivirus).*
3. *<u>Administrative</u> safeguards (i.e. policies, procedures, training, pledges).*

Officials indicated that there is much uncertainty regarding the intent of the PHIA audit requirements. The Department assists regional health authorities and other healthcare entities interpret various aspects of PHIA (e.g. auditing of user activities), but they have not developed guidance for trustees on how to interpret PHIA's audit requirements. Such guidance could include what an audit entails and which security safeguards trustees should audit.

In May 2000 in an effort to ensure compliance with the PHIA audit requirement, the WRHA approved and published its *Audit of Security Safeguards* policy. The policy requires an overall audit of security safeguards, including electronic safeguards, and that a report on the results of the audit is to be prepared by eHealth and the WRHA Chief Privacy Officer every two years. The policy defines an audit as, but not limited to, the following:

- Review of the restrictions on the collection of personal health information, including electronically.
- Review of the effectiveness of the safeguards in place to protect the confidentiality, integrity, and security of personal health information.
- Ensure appropriate policies and procedures are in place to allow only authorized individuals to download or compile personal health information for authorized purposes.

eHealth officials noted that they conduct Threat Risk Assessments when implementing new corporate systems that may be accessed using laptops and desktops, but that they have not audited the effectiveness of their security controls as required by the WRHA policy, including those over end-user devices, nor have the required reports been prepared.

It is important to note that the periodic audit of safeguards required by PHIA and the WHRA policy would likely have identified many of the end-user device control deficiencies we noted in section 2.

Recommendation 6: We recommend that the Department develop guidance for PHIA trustees on how to audit their security safeguards.

Recommendation 7: We recommend that Department monitor trustees' compliance with PHIA's audit of security safeguards requirements.

Recommendation 8: We recommend that the WRHA Internal Audit branch develop and implement a risk-based audit program that would satisfy the requirements of the WRHA's *Audit of Security Safeguards* policy.

3.4 Awareness programs not sufficiently developed

Organizational awareness programs help communicate expectations and ultimately change user behavior, reducing risk. For instance, healthcare organizations implement comprehensive awareness programs to improve hand hygiene – this is critical for patient safety.

Similarly, privacy and security awareness are critical to information security management programs. They enhance a user's ability to recognize weaknesses, incidents and potential breaches. They also educate users on what to do in the event of suspected incidents and breaches.

Well-designed programs use multiple techniques, in addition to face-to-face or online training, to increase awareness within the organization. These could include, but are not limited to, contests, awards, posters, brochures, emails, and other materials (e.g. pens, mouse pads).

WRHA has developed PHIA awareness training for associated individuals (e.g. physicians and medical staff, contractors, students, researchers and employees) that can be accessed in-person, on DVD, or online. In addition, eHealth has developed an online information security training session.

We found, however, that the privacy and information security awareness training courses:

- Are not based on documented risk assessments.
- Are the same for all attendees regardless of the risk associated with job functionality.
- Do not communicate incident handling procedures.

In addition, as detailed below, we found that:

- Attendance is poor.
- Training content is missing important elements.
- Additional techniques are not used for information security awareness.

Attendance requirements and tracking

PHIA	Information Security
PHIA legislation requires that trustees provide orientation and ongoing training to employees and agents (e.g. contractors) on their policies and procedures. The WRHA's Confidentiality of Personal Health Information policy requires attendance to the training within three months of commencement/hiring. However, the policy does not require periodic attendance thereafter. The WRHA does not centrally track or manage attendance. We were unable to obtain a complete listing of all attendees within the WRHA. However, they are implementing a new system to centrally manage attendance and ensure compliance with WRHA policy.	The WRHA does not require employees and agents to attend the information security awareness training. Only 690 WRHA individuals have taken the information security awareness training. Of this total, 620 were from eHealth, leaving only 70 other individuals from within the entire WRHA that have attended the training. We are concerned with the WRHA's extremely low attendance.

Training content

WRHA Policy Requirements	PHIA			Information Security
	In-Person	DVD	On-Line	On-Line
Encryption – End-user devices are required to be encrypted. Personal health information cannot be stored on a smartphone that is not encrypted.	No	No	Yes	Yes
Authentication – End-user devices are required to have strong authentication.	No	No	No	Yes
Transmitting sensitive information – Users are not to transmit sensitive information over the Internet unless appropriately secured.	No	No	Yes	No
Use of personally-owned devices – These devices cannot be used for transmitting, storing or viewing work related information unless configured by Manitoba eHealth with the appropriate safeguards.	No	No	No	Yes

Additional techniques used	
PHIA	**Information Security**
The following additional awareness techniques are in place: • The Department has posted a *Privacy Toolkit for Health Professionals* on their website which includes frequently asked questions, literature from external sources, as well as PHIA summaries for health care professionals, facilities, researchers, agencies, and information managers. • The WRHA website posts privacy policy instruments and also describes privacy officer responsibilities (and their contact information). However, no other privacy related information is included on the site (e.g. Frequently Asked Questions, tips). • Healthcare providers can download a poster and a brochure regarding PHIA directly from the WRHA website. • eHealth distributes privacy related labels (for sticking to computers and screens). • Privacy is noted throughout eHealth provincial system brochures, pamphlets and signage (e.g. eChart, TeleHealth, Electronic Medical Records). • eHealth’s internal site devotes a portion to privacy.	eHealth provides security related information on an internal site (e.g. protection of personal devices, encryption, passwords, and emailing sensitive information) that is available to all WRHA users, including other Regional Health Authorities. However, beyond the training and intranet site, eHealth has not implemented any other additional awareness techniques such as contests, posters, brochures, or other materials (e.g. pens, mouse pads).

Recommendation 9: Upon the completion of risk assessments, we recommend that WRHA update the PHIA and information security awareness training sessions to:

a) Communicate a complete and consistent set of risks, expectations and requirements pertaining to personal health information residing on or accessed by end-user devices.

b) Develop training that specifically targets users in higher risk positions.

c) Outline incident handling procedures.

Recommendation 10: We recommend that the WRHA update the *Confidentiality of Personal Health Information* policy to require that associated individuals (e.g. physicians and medical staff, contractors, students, researchers and employees) periodically attend PHIA awareness training.

Recommendation 11: We recommend that the WRHA require that associated individuals (e.g. physicians and medical staff, contractors, students, researchers and employees) using WRHA information assets attend the information security awareness training upon hiring and periodically thereafter.

Recommendation 12: We recommend that eHealth implement other information security awareness techniques to complement and reinforce the messages communicated in its awareness training courses and intranet site.

Summary of recommendations and responses of officials

Recommendations directed to WRHA/eHealth

Recommendation 1: We recommend that eHealth identify and assess the risks associated with end-user devices used within the WRHA environment.

> Manitoba eHealth agrees, and has already started work on the conduct of risk assessments of end user devices used in the WRHA environment. The results of these assessments will be used to inform and guide implementation of the other OAG Recommendations, and the learnings will be shared with other regions (Regional Health Authorities, CancerCare Manitoba and Diagnostic Services Manitoba) for their reference and benefit.

Recommendation 2: Upon completion of risk assessments associated with end-user devices, we recommend that eHealth communicate the results of the risk assessments to the WRHA Chief Executive Officer (CEO) and that the CEO document the acceptance of residual risks.

> Upon completion of the risk assessments, Manitoba eHealth as part of its ongoing risk management program, and in accordance with WRHA policies, will communicate those risks and applicable mitigating controls to the WRHA CEO for consideration and acceptance. The WRHA agrees that the CEO will review, and if acceptable will document the acceptance of, the residual risks.

Recommendation 3: Upon completing end-user device risk assessments, we recommend that the WRHA implement the controls needed to reduce (to an appropriate level) the risks associated with end-user devices (including the areas of concern noted in our letter to management).

> Upon completion of the risk assessments, as part of its risk management program Manitoba eHealth will identify the additional policies and controls needed to reduce the identified risks to a level acceptable to its stakeholders, and will work with the WRHA on identifying required resulting changes to WRHA Policies and controls.

Recommendation 4: We recommend that eHealth develop a strategic plan for the delivery of ICT services to the WRHA, including plans for remote access through end-user devices.

> As part of its provincial mandate, Manitoba eHealth prepares and publishes annually a provincial eHealth strategy covering the design and delivery of information and communication technology (ICT) services to all Regional Health Authorities. In accordance with the OAG's Recommendation, within a broader provincial strategic plan Manitoba eHealth will create a strategic plan that covers the design and delivery of ICT desktop and infrastructure services specifically for the WRHA. Manitoba eHealth has also commenced work on the development of a strategy for the use of mobile computing,

and in accordance with that strategy will develop plans for remote access through end user devices for the WRHA.

Recommendation 5: We recommend that the WRHA define and implement a structured information classification scheme that includes multiple classifications based on the sensitivity of information.

The WRHA will conduct a risk assessment on the information it holds, and based on that assessment will develop a strategy on how that information is to be classified and handled having regard to its level of sensitivity. This will include a re-examination of the WRHA's extensive current policies applicable to sensitive information, its data classification practices, and its data handling guidelines.

Recommendation 8: We recommend that the WRHA Internal Audit branch develop and implement a risk-based audit program that would satisfy the requirements of the WRHA’s Audit of Security Safeguards policy.

Once it has had the opportunity to consider any guidance that Health may issue for trustees on how to audit their security safeguards, the WRHA will then review and document its existing audit and assessment practices, and then do further work to develop a risk-based audit program which is compliant with it’s Audit of Security Safeguards Policy.

Recommendation 9: Upon the completion of risk assessments, we recommend that WRHA update the PHIA and information security awareness training sessions to:

a) Communicate a complete and consistent set of risks, expectations and requirements pertaining to personal health information residing on or accessed by end-user devices.
b) Develop training that specifically targets users in higher risk positions.
c) Outline incident handling procedures.

The WRHA has already been conducting a review and refresh of its privacy policies and has reminded its personnel of the need to respect and protect the privacy of patients. Upon the completion of the risk assessments, the WRHA will proceed further to implement this Recommendation regarding its PHIA awareness training.

Manitoba eHealth is designing a revised security awareness program that will take into account the results of the risk assessments, as well as an assessment of the target audiences.

Recommendation 10: We recommend that the WRHA update the Confidentiality of Personal Health Information policy to require that associated individuals (e.g. physicians and medical staff, contractors, students, researchers and employees) periodically attend PHIA awareness training.

The WRHA is proceeding to update its policies to require that its PHIA awareness training be taken on a regularly scheduled basis, and is also developing a system to allow it to monitor completion of the training.

Recommendation 11: We recommend that the WRHA require that associated individuals (e.g. physicians and medical staff, contractors, students, researchers and employees) using WRHA information assets attend the information security awareness training upon hiring and periodically thereafter.

> Once the revised security awareness program is made available by Manitoba eHealth, the WRHA will make it mandatory for all of its employees, physicians, and associated individuals who use WRHA electronic information assets to participate, recognizing that the delivery media and vehicles may differ depending upon the target audience.

Recommendation 12: We recommend that eHealth implement other information security awareness techniques to complement and reinforce the messages communicated in its awareness training courses and intranet site.

> The revised security awareness program being developed by Manitoba eHealth will adopt a number of differing awareness techniques, so as to re-enforce the messages being communicated and to address the requirements of the various target audiences.

Recommendations directed to the Department of Health, Healthy Living and Seniors (Department)

Recommendation 6: We recommend that the Department develop guidance for PHIA trustees on how to audit their security safeguards.

> Health will develop and publish guidance for PHIA trustees on how to audit their security safeguards as defined in the Personal Health Information Act. The department will seek to establish an appropriate baseline of safeguards against which to audit; in compliance with acceptable Health Industry sector standards.

Recommendation 7: We recommend that the Department monitor trustees' compliance with PHIA's audit of security safeguards requirements.

> Health will ensure a process is in place to monitor the regions' compliance with the audit of security safeguards requirement.

Auditor General

Norm Ricard

IT Principals

Fraser McLean
Doug Harold

Corporate services

Ken Nero
Shirley Richardson
Shondell Babb
Jim Stephen

Desktop publisher

Shondell Babb

Photographer

Tracey Goncalves

Cover design

Cocoon Branding Inc.

Our contact information

Ofice of the Auditor General
500 - 330 Portage Avenue
Winnipeg, Manitoba
Canada R3C 0C4

Phone:	(204) 945-3790
Fax:	(204) 945-2169
Email:	oag.contact@oag.mb.ca

Copies of this report can be found on our website **www.oag.mb.ca**

Website Version