Innovative Wireless Home Care Services:

Protecting Privacy and Personal Health Information

Information and Privacy Commissioner of Ontario

Soins et Services à Domicile
wecare
Home Health Services

medshare

Healthanywhere
An IgeaCare Systems Company

BlackBerry
Alliance Program

Alliance Members with Research In Motion (RIM)

March 2009

The authors gratefully acknowledge the following staff for their contribution to this paper:

Ken Anderson, Assistant Commissioner, Privacy, Office of the Information and Privacy Commissioner of Ontario, Canada

Michelle Chibba, Director, and her staff in the Policy Department, Office of the Information and Privacy Commissioner of Ontario, Canada

Barbara Toccacelli, Director of Human Resources and Communications, We Care Home Health Services

Amy Morris, Product Manager, MedShare

Shahid Shamsi, Product Manager, Healthanywhere

Information and Privacy
Commissioner of Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Table of Contents

Foreword

Wireless handheld devices have been embraced by businesses and organizations worldwide because they offer increased mobility, efficiency and productivity. Health care organizations are recognizing that this technology can be employed to improve the delivery of patient care. What is particularly exciting is the possibility of wireless mobile solutions being used to support individuals at home, while maintaining ongoing contact with their health care providers. However, privacy concerns associated with wireless handheld devices must be taken into account.

My Office investigated two well-publicized incidents involving wireless and mobile technology in health services. Both incidents underscored the unique privacy-challenging properties of mobile technologies and wireless networks. The risk of theft or loss of a mobile computing device is high – privacy will be breached if personal information stored on the stolen or lost device can be accessed in an unauthorized manner. The wireless transmission of personal information in electronic form means adding another layer of complexity to protect "data-in-motion" as well as "data-at-rest." Any time wireless technology is used to transmit personal information, that information must be strongly protected to guard against unauthorized access to the contents of the signal.

Given the sensitivity of personal health information, unauthorized access can be devastating – especially to someone already dealing with a major health issue. It is critical that there are specific expectations of how such sensitive information is handled and safeguarded. Despite such challenges, I have always believed that technology can be proactively designed to protect privacy, while still delivering functionality and security. Using this approach of "Privacy by Design," society can fully benefit from the many life-enhancing features that this technology has to offer, with the assurance that individual privacy will be protected.

In late 2008, I became aware that We Care Home Health Services (We Care) was piloting wireless mobile solutions involving the use of BlackBerry® smartphones in the delivery of home health care services. I discovered that, in addition to meeting the needs of clients and the organization, a major focus of the BlackBerry® smartphone deployment was to maintain a high standard of privacy protection for their clients' personal health information.

After meeting with We Care, their wireless technology partners, Healthanywhere and MedShare, and Research In Motion (RIM), I was asked to become involved to help provide information to the home care sector, as well as to the wider health care sector, on considering privacy when using wireless handheld devices in the delivery of home health care services.

This paper builds upon previous work that my Office has published in the area of privacy and wireless and mobile technologies. I and my co-authors, John Schram, CEO of We Care, Pramod Gaur, President and CEO of Healthanywhere, and Barry Billings, President and CEO of MedShare, hope that this resource will be helpful to other health sector organizations with a mobile workforce that wish to gain the benefits of wireless technology solutions, and at the same time, protect the privacy of their clients.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario, Canada

I. Introduction

Research demonstrates that information and communication technologies (ICTs) are a critical component to home care service delivery, as they improve health care team communication, innovation and collaboration, and enable easy monitoring of a client's progress.[1] As the demand for health care delivered at one's home increases, driven by the growth of an aging population with chronic diseases, ICTs are increasingly being considered as a means to support the independence of individuals, as well as to enhance the quality and coordination of care.[2]

Wireless handheld devices, in particular, are becoming recognized for the potentially significant benefits they can bring in this regard. This technology offers a practical and affordable solution to the ongoing problem of keeping a large, mobile and dispersed workforce connected with each other and more importantly, connected with one's clients. Clearly, the benefits of wireless communications are many. But, there are also privacy risks. Unauthorized access or disclosure of personal data can occur through loss or theft of a mobile computing device or through unauthorized interception during the wireless transmission of personal data. Without appropriate safeguards, storing personal data on a mobile computing device and transmitting it wirelessly can be like using an open filing cabinet in a waiting room.

It is possible for wireless handheld devices, and other technology deployments, to be both privacy-protective *and* deliver functionality. "Privacy by Design"[3] – a prescient call to organizations in the '90s by one of the authors of this paper, Dr. Ann Cavoukian, Ontario's Information and Privacy Commissioner, helped set the stage for privacy to be built into technology – protecting it from the outset, rather than treating it as an afterthought. Rather than following the conventional zero-sum mindset that privacy can only come at the expense of functionality or security, organizations must recognize that a positive-sum model can be achieved if privacy safeguards are proactively built into a technology or system at the outset. A win-win scenario, whereby privacy, business *and* security interests are served, can and must be achieved. By embracing privacy by design, leading companies have turned their privacy problems into privacy solutions.

This paper provides guidance on privacy best practices for home care organizations when integrating wireless handheld technologies to enhance the efficiency and effectiveness of home care services. It also includes an example of an initiative by We Care and its technology partners, Healthanywhere and Medshare, both Blackberry Alliance Members with Research in Motion (RIM).

1 Canadian Home Care Association, *Integration through Information Communication Technology for Home Care in Canada*, March 2008 p. 9
2 Ibid pp. 6, 12
3 See the IPC's publication discussing the early IPC origins and meaning of the now-popular term "Privacy by Design" at: http://www.ipc.on.ca/images/Resources/privacybydesign.pdf

II. Privacy and Personal Health Information

Privacy laws and regulations across Canada, as well as the day-to-day privacy policies and practices of organizations, are based on fundamental, globally-accepted privacy principles known as "fair information practices." They include the concepts of accountability, specified purposes, consent, data minimization, limited collection, use, retention and disclosure, and safeguards.

In the course of delivering health care to individuals at home, home care organizations and their employees routinely collect and use personal health information (PHI) about their clients, and maintain records relating to this information. Due to the highly sensitive nature of this information, home care organizations should put in place sufficient safeguards (technical, physical and administrative) to protect the privacy and confidentiality of this information, and may be obliged to do so under applicable privacy laws.[4] While clients expect their information to be properly safeguarded, they also expect that it will be shared quickly and accurately among their health care providers to enable the provision of effective and timely care. Health-specific privacy legislation generally provides the required flexibility to allow PHI to be shared among a patient's health care providers for the purposes of providing health care or assisting in providing health care.

In Ontario, the *Personal Health Information Protection Act*, 2004 (*PHIPA*) specifies requirements for health information custodians that relate to these globally-accepted privacy principles. For example, *PHIPA* requires health information custodians to take reasonable steps to ensure that PHI in their custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. *PHIPA* also requires health information custodians to ensure that records of PHI in their custody or under their control are retained, transferred and disposed of in a secure manner.

Personal health information is defined in *PHIPA* to mean identifying information about an individual, either in oral or recorded form falling into one or more specified categories, such as if it:

- relates to the individual's physical or mental health, including family history;
- relates to the provision of health care to the individual, including the identification of persons providing health care;
- is the individual's health number; or
- relates to payment or eligibility for health care, or eligibility for health care coverage, for the individual.

It is important to note that *PHIPA* does not apply to all PHI, but only that which is collected, used or disclosed by health information custodians and certain other persons. To determine whether and how *PHIPA* applies to them, home care organizations should first determine whether they are health information custodians, and they are encouraged to consult their own legal counsel in this regard.

4 Ontario, British Columbia, Alberta, Manitoba, and Saskatchewan have enacted privacy laws that specifically address how organizations handle personal health information in their custody or control.

When considering new ICTs, it is important to recognize that privacy subsumes a set of protections far greater than security. Although building strong security features into a technology is vital to preventing privacy breaches, technological security is only one of the means used to achieve informational privacy.

Information practices are the policies outlining when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of PHI, and the administrative, technical and physical safeguards and practices that the custodian has in place. Developing supporting policies, procedures and an overall culture of privacy ensures that PHI is handled in a privacy-respectful manner by the organization and its employees, whether the PHI is in electronic or non-electronic form.

Privacy is at the heart of user confidence, trust and acceptance of all new technologies, applications and deployments. Organizations that fail to take reasonable steps to ensure that any new technology they deploy sufficiently protects personal information in their custody risk losing the support of the public as well as their good reputation.

III. We Care Home Health Services: Two Wireless Solutions Using BlackBerry® Smartphone

We Care Home Health Services (We Care) is a large home care services provider in Canada, with more than 50 community locations and over 5,000 staff. We Care's services include providing assistance to clients in their homes with activities of daily living, palliative care or managing chronic conditions.

In 2007 and 2008, We Care initiated pilot projects that aimed to integrate wireless handheld technologies in the delivery of home health care services. We Care strongly believes that mobile information technologies, and other ICTs, will play an increasingly important role in making health care accessible to individuals in their homes.

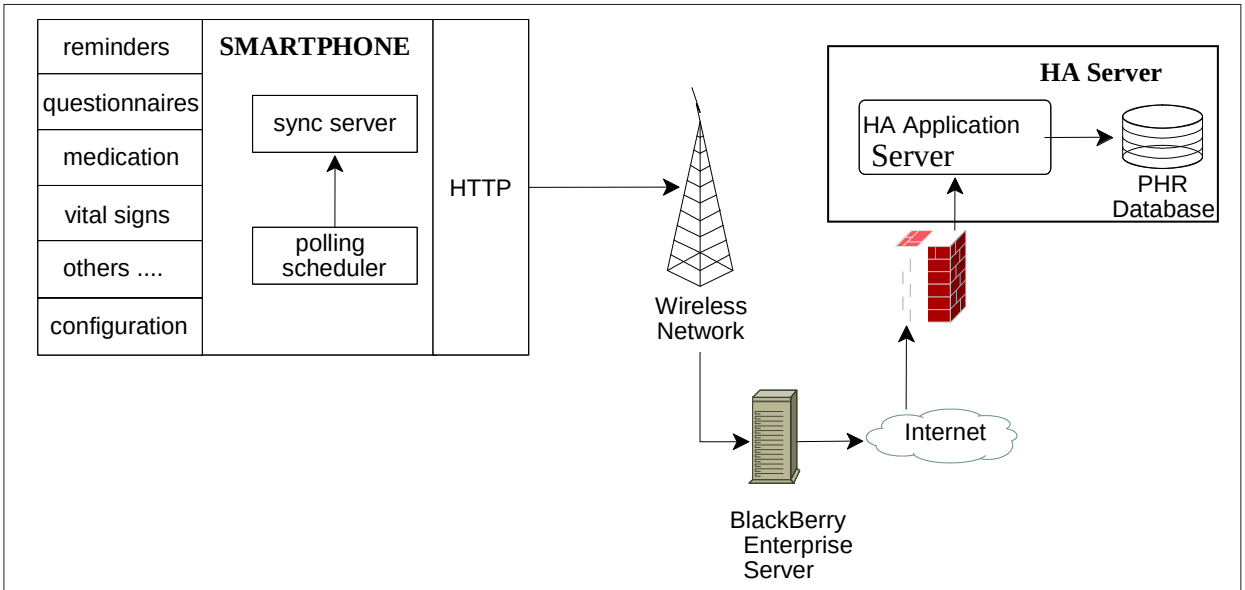
One of the most important benefits that wireless technology provides to We Care's front-line staff and clients is the flexibility of being able to instantly share, access and receive PHI, no matter where they are at any given time. Having real-time information about their clients helps front-line staff to more effectively monitor their clients, and provide quality and appropriate care.

The benefits of wireless technology to clients include: greater independence for individuals with health conditions; easier access to health care for individuals located in remote regions; more empowered clients, as they have the means to self-manage their own conditions more effectively; greater peace of mind for clients and their families, knowing that health care professionals are within close reach; and, enhanced provider effectiveness and safety.

We Care collaborated with wireless health care software providers Healthanywhere and MedShare to design and deploy two wireless solutions using BlackBerry® smartphones. The BlackBerry Enterprise Server (BES) was used as the single platform to support and deliver Healthanywhere and MedShare applications. A core feature of this initiative involves the transfer of PHI wirelessly between members of the home health care team, as well as with their clients. Storage of PHI on the BlackBerry® smartphones, as well as in databases, is also part of the technology solution.

Healthanywhere Solution for the BlackBerry® Smartphone

The Healthanywhere for BlackBerry® smartphone solution (see Figure 1) was designed to help clients with chronic hypertension effectively manage and monitor their condition, while maintaining an active lifestyle. The web-based solution enables We Care staff to monitor in real-time client blood pressure and other vital signs, such as blood glucose, weight and blood oxygen levels, so they may respond quickly when necessary. For example, if blood pressure readings and other vital signs are trending abnormally, We Care staff may send an email to the client's BlackBerry® smartphone reminding him or her to take medications, or take other measures such as notifying the client's physician. The Healthanywhere application also features medication reminders, customized nutrition and exercise plans, and health questionnaires. In addition to hypertension monitoring, We Care anticipates that the BlackBerry® smartphone application will be equally valuable in managing other chronic conditions, and plans to make it available for diabetes monitoring in the near future.



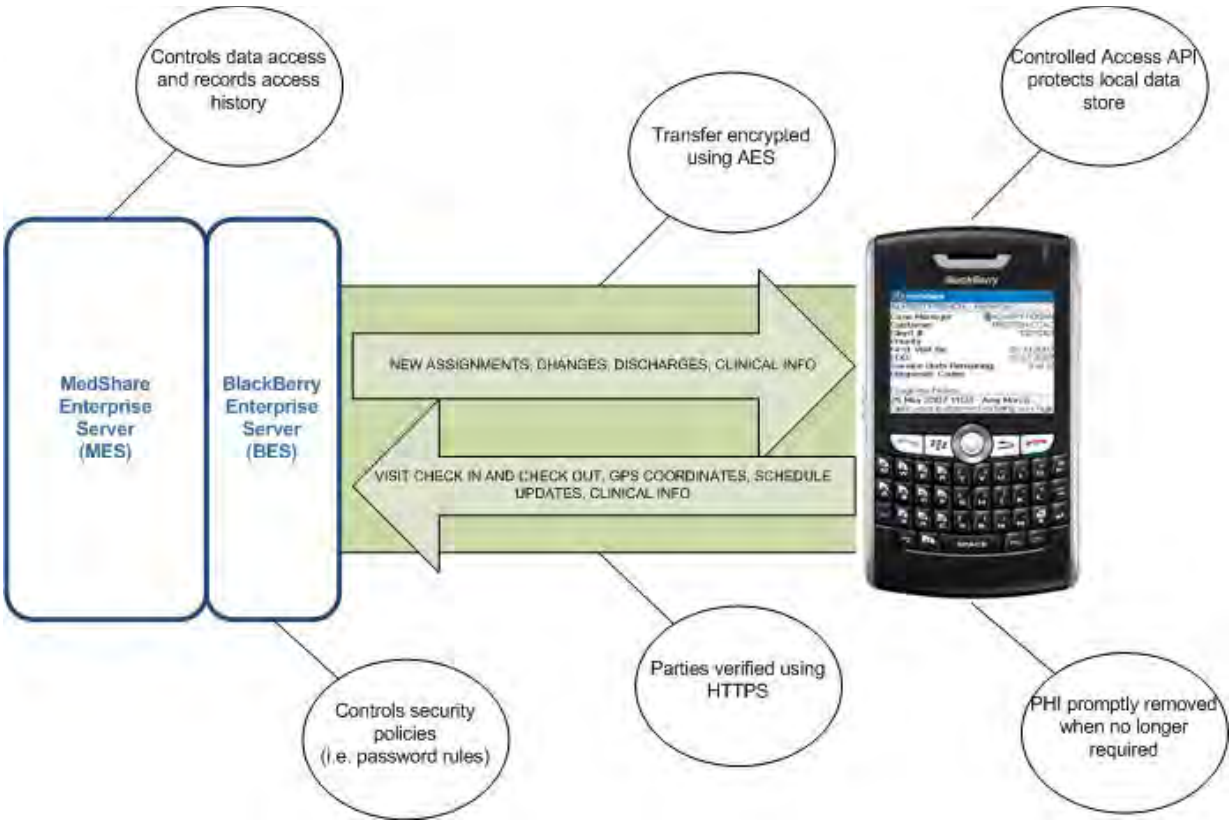
Clients are equipped with Bluetooth®-enabled blood pressure monitoring devices that are paired with BlackBerry® smartphones. When the client measures his or her blood pressure with the blood pressure monitoring device, the reading is sent automatically to the client's BlackBerry® smartphone through a Bluetooth connection. The BlackBerry® smartphone then transmits the reading through the wireless network to Healthanywhere's servers, which hold the repository of clients' electronic health information. The client's profile is then updated to include the new information.

To view and monitor clients' blood pressure readings and other health data, authorized We Care staff log into the Health Care Professional Portal (HCPP) on their computers at We Care offices. The HCPP is the portal through which individuals access client data and profiles held in Healthanywhere's servers. Staff may also access the HCPP outside of We Care offices on any computer with an Internet connection or Web-enabled device.

Figure 1 – Healthanywhere's hypertension monitoring solution for BlackBerry® smartphones

MedShare Solution for the BlackBerry® Smartphone

Replacing a paper and telephone-based system that was labour-intensive and inefficient for We Care's care coordinators and caregivers, the MedShare for BlackBerry® smartphone solution (Figure 2) enables front-line staff to instantly schedule appointments, navigate to treatment sites, confirm arrival and departure times, perform case management and patient charting, and update other members of the home care team at We Care's offices and their colleagues in the field about the client's status. In addition, the MedShare for BlackBerry® smartphone solution allows staff at the point of care to view client electronic health files which reside in We Care servers. The BlackBerry® smartphones also allow front-line staff to quickly reach out to their support network, by email or voice, if assistance relating to the care of a client is needed.



When We Care receives a request for in-home services, We Care's care coordinator schedules the initial visit(s) in their scheduling system. The encrypted information is routed through the BlackBerry Enterprise Server (BES) which resides in We Care offices and is delivered to the BlackBerry® smartphones of scheduled staff. The BES also provides We Care centralized administrative control over security features of the BlackBerry® smartphone. Staff in the field are alerted to the newly scheduled visit(s) by their BlackBerry® smartphones. Staff are able to click on the client's address to get a map or directions to the client's home. The MedShare application stores client information locally on the BlackBerry® smartphone so that it is available even when the device is not receiving a signal. We Care staff can access client data held in the servers by logging into the MedShare application that is installed locally in the BlackBerry® smartphones, or on computers in We Care offices that have the application installed. The servers control access to client data and record access history. The data is automatically removed when no longer required to perform the designated service.

Figure 2 – MedShare's solution for BlackBerry® smartphones

Privacy by Design

Privacy-protective features were engineered directly into the BlackBerry® Enterprise Solution and the Healthanywhere and MedShare applications at the outset.

BlackBerry® Enterprise Solution

- If BlackBerry® smartphones are lost, stolen or left unattended, the BlackBerry® Enterprise Solution offers a number of safeguards to ensure that PHI stored in devices is not accessible to unauthorized persons. We Care's system administrators have the ability to enforce password policies and encrypt data stored in BlackBerry® smartphones, as well as remotely wipe and lock devices using wireless commands.[5] Administrators can also set security timeouts and limit the number of attempts that can be made before their device's memory is erased.

- To ensure that PHI does not remain indefinitely stored in a BlackBerry® smartphone, We Care's system administrators can set IT rules to automatically remove data from the devices after specified periods of time or upon the occurrence of specified events.

- To prevent any interference or interception of data that is transmitted over the wireless network, all data transmitted between the BlackBerry® Enterprise Server (BES) and BlackBerry® smartphone are encrypted end-to-end in accordance with the latest encryption standards, and are authenticated and checked for integrity to ensure that data has not been tampered with nor sent from unauthorized sources. There is no staging area between the server and the BlackBerry® smartphone where the data is decrypted, that could provide an opportunity for unauthorized access in mid-transmission.

- The BES ensures that IT security policies established by We Care's system administrators cannot be overridden by individual users. This ensures that strong privacy protections are applied across all users, regardless of the level of technical knowledge of each user. Additionally, the BlackBerry® solution allows strong central control over the functionality of the BlackBerry® smartphone, preventing unauthorized applications or Bluetooth[6] connections from being established on individual devices to minimize the possibility of malicious attacks being launched from these sources.

Healthanywhere application

- The Healthanywhere application has several safeguards in place to ensure that the transmission of data between the end-user's browser and Healthanywhere's servers is protected. Data travelling through the Bluetooth connection between a client's blood pressure monitoring device and BlackBerry® smartphone is encrypted. The blood-pressure readings travel only as numbers and are not accompanied by any identifiable information, and are only linked with client data once in Healthanywhere's

5 See IPC tip sheet, *BlackBerry® Cleaning: Tips on How to Wipe Your Device Clean of Personal Data*.
6 Bluetooth® technology connects electronic devices using short-range wireless signals. It is used to link mobile phones to headsets, keyboards to mice, and laptops to printers through a "pairing" process.

protected servers. Data that are transmitted to and from BlackBerry® smartphones or Web browser over the wireless network are encrypted. Healthanywhere uses Verisign Secure Sockets Layer (SSL) certificates, which is the same cryptographic system used in many online applications that require the transfer of confidential information, such as online banking applications.

- To ensure that only authorized persons may view client information, members of We Care staff who are authorized to view a client's profile must first log into the Healthanywhere application with a unique username and password. Passwords are regularly changed. Once a session is opened with a valid username and password, only information about clients assigned to the staff are visible. All the sessions are timed out after a brief period of inactivity.

Note that Healthanywhere staff who may need to gain access to client information stored in Healthanywhere's databases in order to provide services to We Care (i.e. technical support) all sign confidentiality agreements.

MedShare application

- All data that is wirelessly transmitted back and forth from BlackBerry® smartphone to the MedShare Enterprise Server (hosted by We Care) is encrypted according to the strongest cryptographic standards. Data that is transmitted from the MedShare Enterprise Server to BlackBerry® smartphones are encrypted using Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES). Data that is transmitted from BlackBerry® smartphones to the MedShare Enterprise Server is encrypted using Secure Sockets Layer.

- To ensure that only authorized persons may gain access to the MedShare application and information stored on BlackBerry® smartphones, users may only unlock the BlackBerry® smartphone by entering a unique password. Strong password policies are enforced by We Care system administrators through the BlackBerry® Enterprise Server. The MedShare application delivers a session token to the device that is required for each information transaction; session tokens expire after a configurable time out, normally set to two hours. The application can only receive updates to client data by either providing this token or providing credentials again to obtain a new token. Once a session is opened, only information about clients assigned to the staff is visible.

- The information stored on the local MedShare for BlackBerry® database is protected through a Controlled Access Application Program Interface (API) preventing other third party applications from gaining access to the data.

While We Care needed to ensure that the BlackBerry® solution offered strong technological security features, it also understood that developing supporting information policies and practices was equally important to ensure that We Care staff handles PHI in a privacy-respective manner. Front-line and office staff are encouraged to de-identify or use pseudonyms, whenever possible, when referring to clients in any email exchanges containing PHI. Staff members are also trained to avoid discussing clients or viewing clients'

information in public places. Furthermore, We Care established policies to remotely wipe client information stored on BlackBerry® smartphones after specified periods, or after it is no longer needed (e.g., scheduling information is wiped every week, emails are wiped every month, a client's information is wiped when he or she is discharged or when staff is no longer assigned to him or her) to reduce the chances of inadvertent disclosure.

IV. Privacy Best Practices for Integrating Wireless Handheld Devices in the Delivery of Home Care

Wireless handheld devices hold enormous appeal for home care organizations that wish to address the challenge of keeping mobile workers up-to-date and connected with each other, and enhancing support for their clients at home. However, home care organizations that are considering using wireless handheld communication devices to transmit PHI should only do so if strong privacy protective precautions have been taken. It is important to recognize at the outset that wireless handheld technologies pose a clear risk to privacy if the proper precautions are not taken. In contrast to wired solutions which do not broadcast data across open air waves, wireless communication technologies transmit data across many frequency bands, and are thus susceptible to interference and interception. Additionally, handheld devices store data, which may be accessed by anyone, if the devices are not properly secured in the event of theft or loss.

Under *PHIPA*, the Information and Privacy Commissioner's Office of Ontario, Canada (IPC) has issued Health Orders that provide guidance to the health care sector on the use of wireless communication technologies and mobile computing devices. In Health Order HO-004,[7] the IPC established expectations for health information custodians covered under *PHIPA* that use mobile computing devices to store PHI. The Order was made following an investigation into an incident that involved the theft of a laptop computer containing the PHI of current and former patients of a hospital. Health Order HO-005[8] demonstrated that wireless communication technologies are inherently vulnerable to interference and interception if strong privacy-protective precautions are not taken. HO-005 reported on an incident where sensitive video images of patients at a clinic were inadvertently intercepted because the clinic had installed a wireless surveillance camera without adequately protecting the wireless transmissions. Both of these Orders resulted in the requirement for health information custodians to apply strong encryption to all personally identifiable health information.

However, it is important to recognize that privacy subsumes a set of protections far greater than security. While building strong security features into a technology is vital to preventing privacy breaches, technological security is only one of the means used to achieve privacy. Organizations must develop supporting policies, procedures and an overall culture of privacy to ensure that personal information is collected, used, disclosed, retained and disposed of in a privacy-respective manner, whether the information is in electronic or non-electronic form.

7 See Order HO-004 at: http://www.ipc.on.ca/images/Resources/up-ho_004.pdf.
8 See Order HO-005 at: http://www.ipc.on.ca/images/Findings/up-ho_005.pdf.

These Health Orders highlight that a multi-layered approach is needed to protect PHI when using mobile and wireless technologies. Prior to deploying wireless handheld solutions, it is important for home care organizations to take the following best practices into consideration, in addition to their existing privacy practices:

1. Privacy impact assessment and threat risk assessment

It is important that home care organizations ask technology providers, including any third-party application vendors, the right questions in order to confirm that PHI will be transmitted, accessed and stored in a secure manner.

These questions are commonly included in a Privacy Impact Assessment (PIA) and Threat Risk Assessment (TRA). A PIA is a tool designed to assist organizations to identify and mitigate potential privacy risks that may occur in the course of operating a proposed or existing information system, technology or program. A TRA identifies information technology system threats, vulnerabilities and possible safeguards and mitigation strategies. The IPC developed guidelines for conducting a PIA[9] as a self assessment tool to assist health information custodians under *PHIPA*. A PIA has become a standard part of the "best privacy practices" undertaken by many organizations in the health sector.

2. Data minimization

The design of wireless solutions in the delivery of home health care services should begin with non-identifiable interactions and transactions as the default. IPC Order HO-004 advises that the first line of defence against unauthorized access is to avoid storing PHI on mobile computing devices at all.

Whenever possible, PHI stored on wireless devices should be de-identified to ensure that if the device is accessed by unauthorized persons, specific individuals' PHI will not be exposed. If the information is coded, the code that is needed to reveal the identities of individuals should be separately stored in a more secure computing device, such as a central server in a facility. In addition, whenever possible, PHI that is transmitted should be de-identified so that in the event the signal is intercepted, the information cannot be used to identify an individual. Wireless handheld solutions may offer an added security feature whereby PHI is transmitted separately from identifiable information about an individual.

If having identifiable PHI on the wireless device is required, then the amount of such PHI should be kept to a strict minimum and for the minimal amount of time necessary to complete the work.

Where PHI must be transmitted or accessed by front-line staff, only the minimal amount of information necessary should be transmitted. To minimize the inadvertent disclosure of PHI, access to a client's information, and sharing of this information among staff, should be restricted to those who are assigned to providing care or services to the client, and should be made available only to the extent necessary to provide the services.

9 See IPC publication, *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act* (October 2005)

3. Encryption

End-to-end encryption of all data transmissions over wireless networks is critical to keeping PHI secure. In the event PHI is stored on wireless handheld devices, the information *must* be encrypted. Encryption of data prevents unauthorized parties from accessing PHI stored in handheld devices, even if a device is lost or stolen.

Because home care organizations would be responsible for a substantial number of handheld devices, giving individual users the discretion to implement any one of a variety of encryption options is not advised. Home care organizations should look for wireless handheld solutions that provide system administrators central control over encryption standards and enforcement. As encryption standards are continually evolving, organizations should ensure that they choose proven encryption techniques to ensure that PHI is appropriately secured.

At the time of writing, Advanced Encryption Standard (AES) was recommended for the secure storage and transmission of data, and is widely used throughout government and financial sectors. An encrypted tunnel may also be used as a secure method for data transmission. This is generally established through a Secure Socket Layer (SSL) protocol, which is used in many online applications, such as Internet banking.

4. Data integrity

To establish confidence that PHI has not been tampered with or altered during transmission, wireless handheld solutions should include mechanisms to prevent and detect any changes or modifications of data.

5. Data authenticity

Data authenticity allows the recipient to trust that a message was not sent by an unauthorized party that is pretending to be an authorized user or handheld device. To prevent this from occurring, a wireless handheld device should be required to authenticate itself to the network and enterprise systems, and the enterprise server should authenticate itself to the device.

6. Control over third-party applications and Bluetooth® connections

To prevent malicious third-party applications from being downloaded onto wireless handheld devices, which may be designed to steal data, gain access to the organization's network or cause harm to the network, the wireless solution should allow system administrators to control or block the installation of third-party or untrusted applications.

Bluetooth connections between Bluetooth-enabled wireless handheld devices and other Bluetooth devices may pose similar privacy and security risks. Bluetooth technology connects electronic devices (i.e,. mice to keyboards, mobile phones to headsets, etc.) using short-range signals, eliminating the need for cables. Although security options are available, some of these systems are not fully secure. Organizations that are considering the use of Bluetooth technology should take special precautions to reduce Bluetooth-specific vulnerabilities.

The Bluetooth function on devices containing or having access to PHI should not be turned on without confirming that the connection is, in fact, secure and protected. If devices are being used to transmit PHI, wireless handheld solutions should allow system administrators to enable and disable Bluetooth functionality at the device level, control which devices can connect using Bluetooth technology, and ensure that the Bluetooth-enabled devices are not set up to broadcast data unprompted.

7. Other safeguards

A wireless device in the possession of front-line staff or clients can store PHI temporarily or for longer periods to allow users to view the information locally. If the device is lost or stolen, or is left unattended, PHI stored in the device could be accessed by unauthorized persons if the appropriate safeguards are not implemented.

In addition to encryption, other features, such as strong passwords, data wiping, locking, and security timeouts, should be employed to ensure that only authorized persons can access PHI stored in devices. Home care organizations should search for wireless solutions that allow corporate system administrators to enforce and have full control over device-level security features, ensuring that they are applied consistently across all devices and cannot be overridden by individual users.

The security policies and features that system administrators should be able to enforce remotely include:

- mandatory password authentication/power-on passwords;
- password length and composition;
- password expiration;
- the number of password attempts on the device before data on the device is deleted;
- security timeouts that set the number of idle minutes before the device locks;
- periodic challenges that will require the user to enter a password a certain period of time after unlocking the device;
- wiping/erasing of device contents;
- locking of devices; and
- resetting of passwords.

8. Limiting retention and secure destruction

PHI that is stored on the device could remain there indefinitely, increasing the opportunity for inadvertent disclosure, if there is no practical means to remove the information

when it is no longer needed. PHI should be retained on handheld devices only as long as necessary. To minimize privacy risks, home care organizations may wish to consider specifying a limited length of time PHI can be retained in wireless handheld devices, before it is automatically deleted.

Once staff are no longer assigned to the client, or the client is discharged, access to the client's PHI should be removed, and the client's PHI that is stored in handheld devices should be wiped. Staff should be encouraged to delete any PHI on their devices as soon as it is no longer required for the purposes of providing services. Moreover, system administrators should be able to identify all PHI stored in a handheld device in the event of a possible privacy breach whereby the device is lost, stolen or its contents are accessed by unauthorized persons.

Once a decision has been made not to retain or archive PHI, PHI should be disposed of in a secure manner, whether it be in paper or electronic format. Secure destruction of personal information contained in wireless handheld devices typically means physically damaging the device and discarding it, or wiping the device if it is to be reused. The IPC's fact sheet, *Secure Destruction of Personal Information* provides further guidance on how to securely dispose of PHI. Another IPC resource is, *BlackBerry® Cleaning: Tips on How to Wipe Your Device Clean of Personal Data*.

9. Regular audits

Once the wireless handheld solution is installed, the home care organization should establish a schedule for objective and comprehensive privacy (including security) reviews appropriate for the system involved. For home care organizations that fall under *PHIPA*, failing to conduct regular reviews of their information technology from a privacy and security perspective is likely to fall short of meeting the reasonableness standard under the Act with respect to their requirement to protect PHI.

10. Privacy policies and procedures

Privacy policies and procedures should comprehensively outline the home care organization's information practices, which address areas such as assigning accountability for privacy to specified individuals, defining the purposes for which personal information is collected, and outlining the organization's procedure for responding to privacy breaches.

Because of the varying degree of technical knowledge of staff and clients, the privacy-protective features on the wireless devices may not be employed consistently for all users (i.e., strong passwords, encryption of data, etc.), or users may not understand all of the privacy vulnerabilities to which wireless handheld technologies are susceptible. To ensure that all staff who are assigned wireless handheld devices are aware of and understand the privacy policies and procedures relating to the wireless applications, ongoing training and education should be provided to them.

Policies should address front-line staff accessing and viewing client health records on wireless handheld devices in public places. Such instances could provide an opportunity for "shoulder surfing" to occur. Staff may also engage in conversations

with their colleagues or clients using their BlackBerry® smartphones, and any discussions involving a client's PHI could inadvertently be heard by others nearby.

Home care organizations should also clearly define roles and responsibilities for privacy and security, and establish who is authorized to access PHI for which purposes. Access to PHI must be restricted to clients and We Care staff who are currently assigned to provide direct health care or assist in the provision of health care to the client. Control mechanisms ensure that only authorized staff and individuals have access to PHI, and that they are handling the PHI in a privacy-protective manner.

If external technology providers are engaged to provide wireless services, home care organizations should ensure that these providers have established their own privacy and security rules that set out policies and procedures for their own staff. These should include requiring staff to sign confidentiality agreements, and defining who is authorized to access PHI and under what circumstances.

V. Conclusion

As innovations in wireless applications develop, wireless handheld devices will present innovative new ways to improve the delivery of health care in one's home. However, in order for home care organizations, their staff and their clients to fully benefit from wireless applications, it is critical for organizations to understand and address the unique privacy threats that wireless solutions present. Working in conjunction with RIM, Healthanywhere and MedShare, both BlackBerry® Alliance Members with Research In Motion (RIM), We Care Home Health Services has demonstrated that it is possible to deploy wireless handheld solutions that provide the functionality required to enhance client care, *and* protect client PHI.

To ensure that PHI being transmitted or stored in handheld devices is sufficiently protected, it is vital that technological security features, such as data encryption, password enforcement and device wiping, are embedded into the wireless handheld solution that is selected. Home care organizations should engage in a discussion with technology providers about their legal responsibility to protect PHI, in order to determine which solution would best meet their needs. Privacy-respectful practices, such as minimizing the storage and retention of personal data, will also reduce potential privacy risks. Home care organizations should develop and establish supportive privacy policies, practices and an overall culture of privacy to ensure that people and processes are handling PHI in a privacy-protective manner throughout the entire information life cycle.

Wireless handheld devices can present new challenges to privacy, however, these challenges can be addressed if privacy practices and safeguards are proactively built into the design of these wireless solutions.

References

Canadian Home Care Association

Canadian Home Care Association. (2008) Integration through Information Communication Technology for Home Care in Canada, retrieved from http://www.cdnhomecare.ca/media.php?mid=1840.

IPC Resources

All resources listed below are available on the IPC's website: www.ipc.on.ca.

A Guide to the Personal Health Information Protection Act at: www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=400

Health Information Custodians Working for Non-Health Information Custodians at: www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=457

Wireless Communication Technologies: Safeguarding Privacy & Security at: www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=645

HO-004 *(Health Order regarding a stolen laptop computer containing personal health information* at: www.ipc.on.ca/english/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=7616

HO-005 *(Health Order regarding inadvertent interception of video images of patients captured by a wireless surveillance camera)* at: www.ipc.on.ca/english/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=7690

Safeguarding Personal Health Information at: www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=181

Secure Destruction of Personal Information at: www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=451

Encrypting Personal Health Information on Mobile Devices at: www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=613

Safeguarding Privacy in a Mobile Workplace; Protect the information you keep on your laptops, cellphones and PDAs at: www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=628

Reduce Your Roaming Risks: A Portable Privacy Primer (Keep it to Yourself) at: www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=465

BlackBerry® Cleaning: Tips on How to Wipe Your Device Clean of Personal Data at: www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=810

Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act at: www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=574

Research In Motion

Website: www.blackberry.com/healthcare and www.blackberry.com/security

Healthanywhere Inc.

Website: www.healthanywhere.com

Address for privacy related enquiries: privacy@medshare.com.

MedShare

Website: www.medshare.com

MedShare for BlackBerry Privacy and Security (available upon request, at info@medshare.com).

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
CANADA

Telephone: (416) 326-3333
Toll-free: 1-800-387-0073
Fax: (416) 325-9195
TTY (Teletypewriter): 416-7539
Website: www.ipc.on.ca
E-mail: info@ipc.on.ca