

Bell EMR Privacy and Security Policy
Updated November 2011

At Bell, we take steps to ensure that the personal health information we hold on behalf of our customers – the physicians of Ontario – is protected in accordance with applicable privacy laws, and to enable physicians using our services to meet their privacy obligations to their patients.

This Privacy and Security Policy document describes the privacy and security steps taken by Bell, and the privacy responsibilities and obligations of physicians subscribing to Bell EMR services, with respect to personal health information input and stored through the Bell EMR system.

Bell EMR ASP Service

An Application Service Provider (ASP) is an organization that manages and distributes software-based services and solutions to customers across a wide area network from a central data centre.

An EMR (electronic medical record) is a suite of software that enables physicians to manage their practices more efficiently by providing them with electronic means for billing for services, for registering patients and for scheduling patient appointments. An EMR also provides physicians with the means to move from paper medical records to electronic records. Electronic medical records provide physicians with quick access to a patient's critical information.

Under an agreement with OntarioMD (www.ontariomd.com), which is a subsidiary of the Ontario Medical Association (www.oma.org), and eHealth Ontario (www.eHealthOntario.on.ca), which is an agency of the Ontario Ministry of Health and Long Term Care, Bell provides EMR services to Ontario health care providers.

As an ASP, Bell EMR (www.xwaveEMR.com) manages the electronic medical records information system where subscribing Ontario physicians record and store their patients' personal health information. This means that Bell is responsible for installing, operating and managing the necessary computer equipment at the eHealth Ontario data centre and for managing and maintaining the Bell EMR software. The ASP service is intended to permit authorized people to have access to the EMR virtually 24 hours per day, 7 days per week, and to enable patient medical records to be available to physicians whenever they are needed.

Personal Health Information Protection Act (2004)

As a provider of services to permit health care providers to use electronic means to collect, use, disclose, modify and retain personal health information, as described in Ontario's Personal Health Information Protection Act (PHIPA) regulations, Bell has implemented safeguards to protect the confidentiality of patient personal information that is collected through the Bell EMR system and stored in the eHealth Ontario data centre.

Pursuant to applicable regulations under PHIPA, Bell takes steps to:

- Notify the responsible health care provider of any privacy breaches;
- Perform risk and privacy assessments;

- Provide an audit trail;
- Ensure that third parties engaged by Bell to perform the Bell EMR services on its behalf comply with applicable restrictions on the use and disclosure of personal health information;
- Make publicly available information about the Bell EMR services to the custodian.

Additional information on PHIPA can be found at www.health.gov.on.ca or www.ipc.on.ca.

Security Safeguards to Protect Personal Health Information

Under PHIPA, personal health information is required to be protected against loss, theft or unauthorized use or disclosure. Bell and its EMR service employees and subcontractors take reasonable steps to maintain the privacy and confidentiality of the personal health information input and stored through the Bell EMR service.

Security safeguard measures Bell uses to protect personal health information input and stored using the Bell EMR service include:

- threat risk assessments
- password policies
- user identity verification and access controls
- tracking accesses and attempted access to patient information
- monitoring of potential and actual system security breaches
- firewalls and virus protection
- server hardening, patch management, change management and system logging and monitoring
- staff security clearance policies and procedures
- other physical, technical, operational and administrative controls and procedures

The physician is the custodian of his/her patients' electronic information. The Bell EMR software is designed such that access to patient information requires the use of confidential usernames and passwords, known only to the individual physician and staff he/she has authorized to have access. Each authorized user is able to see only what the physician permits them to see. See below for more information about the physician's security responsibilities.

What are Bell EMR privacy and security practices? What are the physician's privacy and security responsibilities with respect to personal health information?

While Bell does not have any personal health information in its custody or control, it is responsible for the maintenance of the Bell EMR services, which include privacy and security measures, on behalf of the primary care physicians and their patients. As such, Bell has designed the functionality of the EMR services with the objective of ensuring that both Bell, as the service provider, and your physician, as the health information custodian, are able to meet the requirements of PHIPA to protect the privacy and confidentiality of personal health information stored and processed through the Bell EMR services.

Bell has developed the following policies that provide employees and subcontractors with rules for protecting the privacy of personal health information according to the requirements of PHIPA. It is based on the ten fair information principles described in the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information, which forms the basis of the federal Personal Information Protection and Electronic Documents Act (PIPEDA). The following also describes the privacy and security responsibilities of the physician and other users of the Bell EMR service.

Principle 1: Accountability

Bell has a privacy office that is responsible for the compliance of the Bell EMR services with Bell's privacy policies. This office oversees Bell EMR services privacy requirements, employee and subcontractor compliance with Bell EMR-related privacy policies, and the development and maintenance of Bell EMR-related privacy procedures.

Principle 2: Identifying Purposes

Bell provides reasonable functionality within the Bell EMR services intended to enable physicians and their support staff to identify and document the purpose of the collection of an individual's personal health information prior to or at the time the information is collected. It is the physician's responsibility to ensure that the purposes of collecting personal health information are identified to his or her patients as required by PHIPA or other applicable privacy laws.

Principle 3: Consent

Bell provides reasonable functionality in the Bell EMR services for the physician and their support staff to obtain and document an individual's consent (or withdrawal) for the collection, use or disclosure of their personal health information. It is the physician's responsibility to ensure that appropriate consent is obtained for the collection, use and disclosure of personal health information as required by PHIPA or other applicable privacy laws.

Principle 4: Limiting Collection

Bell endeavors to provide Bell EMR system functionality intended to assist health information custodians with the ability to limit the collection of personal health information to what is required by them to provide health care services to the patient. It is the physician's responsibility to ensure that the collection of personal health information is limited to that which is reasonably necessary to meet the purpose for which it is collected as required by PHIPA or other applicable privacy laws.

Principle 5: Limiting Use, Disclosure and Retention

Bell provides EMR system functionality intended to assist physicians and their support staff in preventing unauthorized use and disclosure of personal health information. Bell uses reasonable measures to prevent unauthorized access to personal health information by Bell employees and subcontractors. Policies and procedures relating to breaches of privacy, security and confidentiality of an individual's personal health information in connection the Bell EMR services are in place. It is the responsibility of the physician using the Bell EMR services to ensure that the use and disclosure of personal health information stored through the physician's account or the accounts of his/her support staff is limited to what is reasonably necessary to meet the purposes for which it is collected and is otherwise in compliance with PHIPA and other applicable laws. Where reasonably possible, Bell will ensure that Bell EMR service functionality includes authorization procedures for accessing personal health information that includes a protocol for tracking who accessed the information and for what purpose.

The Bell EMR system includes functionality intended to support the physician's observance of retention and destruction periods with respect to personal health information. It is the physician's responsibility to ensure that legal and regulatory requirements and professional obligations regarding personal health information and medical record retention are adhered to.

Principle 6: Accuracy

Health information custodians who collect, use and disclose personal health information retained within the Bell EMR system will be responsible for ensuring and maintaining its accuracy.

Principle 7: Safeguards

The Bell EMR service incorporates reasonable safeguards, including technological measures (e.g., the use of passwords and access controls), to protect personal health information stored and processed using the Bell EMR system against loss or theft, as well as unauthorized access, use, disclosure, modification or destruction. See the section above entitled "Security Safeguards to Protect Personal Health Information" for more information about Bell's security practices. Security responsibilities of physicians and other users of the Bell EMR system include:

- protecting usernames and passwords assigned to or selected by the physician and his/her support staff, and ensuring usernames and passwords are not disclosed or shared by or between users within or outside of the physician's office
- immediately notifying Bell in the event of password theft, leak or other compromise
- using secure tokens or other security safeguards as directed by Bell from time to time
- ensuring that computers used to access the Bell EMR service are located in a secure area within the physician's office
- not storing personal health information or other sensitive data on removable media, such as CDs, USB drivers or diskettes
- ensuring that operating system patches and anti-virus software are installed and up-to-date on all computers used to access the Bell EMR service
- complying with other reasonable security policies established and communicated to the physician and other users from time to time.

Principle 8: Openness about Policies and Practices

Bell provides this Privacy Policy document regarding the Bell EMR services in order to make information about the service and Bell's privacy policies and practices readily and easily available to individual physicians and others. For further information about Bell's privacy policies and practices relating to the Bell EMR services, physicians and other users of the service can contact the Bell privacy office as follows:

**Privacy Officer
Bell EMR
Bell Canada
1550 Enterprise Road, Suite 100
Mississauga, Ontario L4W 4P4**

Principle 9: Individual Access

The health information custodian has responsibility for providing individuals with information about the existence, use and disclosure of their personal health information and providing access to that information as required in accordance with PHIPA and other relevant privacy laws. Bell will not provide individuals with access to or copies of their personal health information, and will refer all such inquiries to the responsible subscribing health information custodian. The Bell EMR service functionality is designed to support means to enable the subscribing health information custodian to provide to individuals with appropriate access to their personal health information stored on the Bell EMR system.

Principle 10: Challenging Compliance

Bell does not have custody or control of personal health information and can only respond to inquiries regarding its privacy policies and obligations under applicable legislation. It is the responsibility of health information custodians who have custody and control of personal health information to respond to challenges concerning compliance with the above principle, as it relates to their respective services. Bell will develop procedures to receive and respond to complaints or inquiries from subscribing physicians about its privacy policies and practices with respect to the Bell EMR services.

For more information about the Bell EMR services provided by Bell, visit our web site at: <http://www.xwaveEMR.com> or contact:

**Bell EMR
Bell Canada
1550 Enterprise Road, Suite 100
Mississauga, Ontario L4W 4P4
Phone: (905) 670-1225
Fax: (905) 670-2903**