October 13, 2016

KEEPING PATIENT DATA IN EMRs PRIVATE

Protecting the privacy of personal information is a fundamental right of individuals and a principle enshrined in Canadian law. OntarioMD takes the privacy and security of patient data stored in electronic medical records (EMRs) very seriously. EMRs contain a rich array of personal health information (PHI) and personal information (PI). This information is critical to the provision of care to patients. As the foremost authority on EMRs in Ontario, OntarioMD has worked with physicians and EMR vendors to ensure that the EMRs it certifies through its comprehensive, industry-leading EMR Certification and Specification Programs, are responsive to the requirement that the privacy and security of PHI and PI be an absolute requirement.

Under current Ontario privacy legislation, i.e., the *Protection of Personal Health Information Act* (PHIPA), physicians are Health Information Custodians (HICs) and EMR vendors are not. EMR vendors are service providers to HICs and have no right to use PI contained in the EMR for their own purposes or for any purpose beyond providing their EMR offerings and are further prohibited from disclosing PI. Under the Act, HICs are responsible for the data in their EMRs and there are privacy laws and regulations in place which provide clear direction on how this important information may be accessed and used by the HICs. An EMR vendor in Ontario may not access and use information contained within an EMR without the explicit authorization of the HIC in accordance with applicable law and appropriate consent of the patient.

ONTARIOMD'S EMR CERTIFICATION PROGRAM

To help physicians protect against unauthorized use or disclosure of PI, OntarioMD requires that the EMRs it certifies (both Local and ASP/hosted) through its EMR Certification Program do not allow their respective EMR vendors or any other unauthorized person to access patient data stored in EMRs.

OntarioMD's EMR Certification Program includes compliance with current applicable EMR Specifications in Ontario and compliance with the EMR Agreement between OntarioMD and every EMR vendor that has a certified EMR offering. The EMR Agreement's terms require that the EMR vendor comply with PHIPA and all applicable privacy legislation and regulations. Under the agreement's terms, the EMR vendor "will comply with the restrictions on the access and use of PHI in the Regulations and the prohibition on disclosing PHI and will use Personal Information only to the extent required to provide its EMR Offerings and will not disclose Personal Information".

In addition to the requirement to comply with PHIPA and all applicable regulations, the EMR Agreement between each EMR vendor and OntarioMD also states that the vendor shall "describe the administrative, technical and physical safeguards that the Vendor and its EMR Offerings employ to protect the confidentiality, integrity and security of PHI" and "the Vendor will not enter into any agreement, arrangement or plan to acquire, use or disclose or obtain or exercise, for its own benefit, any rights in all or any portion of the Data or proprietary information of clients, whether or not pseudonymized". Pseudonymization is a procedure by which

the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.[1]

Finally, another important requirement to ensure EMR vendors fulfill their privacy obligations is the need to designate a Privacy Officer who oversees the vendor's compliance with the terms of the EMR Agreement.

FOR MORE INFORMATION:

If you have questions not addressed in this bulletin, OntarioMD is at your service. Please contact your OntarioMD Practice Management Consultant or info@ontariomd.com.

---

[1] Wikipedia, https://en.wikipedia.org/wiki/Pseudonymization