New PHI requirements tabled for Health Sector

- EHR governance inches closer in Ontario

Ontarians are one step closer to the realization of a *"safe and secure electronic health record (EHR)",* as Bill 78**,** the Electronic Personal Health Information Protection Act 2013 moved into the Second Reading in the legislature. The commitment by the Minister of Health, Hon. Deborah Matthews, is to have all **Personal Health Information (PHI)** protected by 2015.

The **Electronic Personal Health Information Protection Act 2013**, first introduced in May, seeks to provide an enhanced system of governance for all Electronic Health Records. Bill 78 expands the obligations for PHI and doubles the fines for violation.

The Bill sets out a series of obligations for Prescribed Organizations (PO), defined as any organization that *"administer, create, integrate, manage, maintain or service an electronic health record"* or conduct analysis of PHI of any sort. This expanded definition would include all Health Care Facilities (HCF), Case Managers, PMS and other software vendors providing database, scheduling, clinical notes or analytical solutions to HCFs and Custodians.

The set fines have been increased to $100,000 for an individual and up to $500,000 for an organization found guilty of a PHI violation. A PO will be obligated to notify the Commissioner immediately, in writing, of any PHI violations.

The obligations of POs under the proposed bill are quite comprehensive. Here are three new requirements that would have significant impact on all POs, especially Health Care Facilities.

- A PO will have to keep a *"detailed electronic log of all instances where all or part of the PHI is viewed, handled or otherwise dealt with; or transferred to the custodian."* This requirement has significant implications for Healthcare companies, especially those that are using a multitude of software such as Google, Dropbox, online scheduling, Access, Excel and other non-compliant programs. The options are either -
    - To maintain a manual log of all the PHI activity which is time consuming and onerous.
    - Invest in a PMS program bearing a full audit trail system. Many older PMS programs do not have the benefit of an audit trail system.
- A PO must be able to "*track an individual's withholding or withdrawal of all or part of his or her consent to the collection, use and disclosure of his or her PHI*." This "lockbox" concept has been in place for some time now but is foreign to most PMS software.

- A PO must "*protect the integrity, security and confidentiality of the PHI.*" This requirement includes all electronic sharing or transference of PHI to third parties. Currently, most medical reports are transferred to payers such as insurance companies, WSIB, CCAC, lawyers or other medical professionals via fax and email. Neither of these methods of transfer meets the test for security and confidentiality. To meet the proposed requirements, Health Providers and other POs will have to use a Secure File Transfer program to transfer or share PHI with third parties.

The security and confidentiality of the PHI can be achieved, in part, through the use of a data encryption process, both in transmission and while at rest. The recent loss of 18,000 records, by a Peel Region Health Service employee, highlights the vulnerabilities of unencrypted data. It is no secret that thousands of Health Care Facilities and Health Providers have unencrypted data stored on computer drives, back-up disks, unsecured online drives and memory sticks. Many of these vulnerable data storage are disasters waiting to happen.

The goal set by the Hon. Deborah Matthews to have all PHI protected by 2015 is highly commendable. It is, without a doubt, a tall order that would require a proactive position by the various colleges, the privacy commission and the investment of significant resources by both public and private sector organization.

A responsible attitude by POs should be to start looking at the implications of this proposed legislation. Meeting these new requirements may involve upgrading to a compliant system, which can be costly if left for the last minute.

About the Author

Danny Doobay has been a Business and IT consultant to industry and government for more than 25 years. He has held executive positions in both public and private sectors.   He has also project managed software development, implementation and data migration.

He is currently the CEO of Baylaan Technologies, a software solutions developer based in Markham, Ontario. Baylaan develops both custom and packaged software solutions for several sectors, including the increasingly popular SkeduleX Practice and Case Management System.

Danny Doobay, MBA, BA (Hons.)
Chief Executive Officer
Baylaan Technologies Inc.
Tel: 905-202-4716
Email: ddoobay@baylaan.com
http://www.baylaan.com/

Follow Danny on: