Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Efficiency in Health Information Systems: Calculating Privacy As Part of the Equation

Patricia Kosseim, General Counsel

Office of the Privacy Commissioner of Canada

Remarks to the Canadian Academy of Health Sciences, Chateau Laurier, Ottawa

September 15, 2011

Introduction

The debate about privacy in the health sector has evolved over the past decade…

- From a focus on informed consent and the need for harmonized rules, towards greater recognition of trust and accountability as critical conditions for success of the EHR endeavor.

- From fear-mongering about hypothetical data breaches to the current reality where data breaches do happen and need to be proactively managed.

FRONT PAGE NEWS

www.dailynews.com THE WORLD'S FAVOURITE NEWSPAPER - Since 1879

Risks of data breach are "top of mind" for Canadians

A Google search for "Sony data breach" reveals almost 38,000 pages in Canada. That figure increases to 1.48 million pages worldwide.

The Epsilon breach reveals 184,000 pages worldwide and over 3000 in Canada.

65% of Canadians believe that protecting personal information of Canadians will be one of the most important issues facing the country in the next ten years.
(Harris Decima public opinion survey, 2011)

Data Breach Notification: Where the law stands in Canada

Ontario *Personal Health Information Protection Act* 2004, subsection12*(2)*
A health information custodian shall notify individuals at the first reasonable opportunity if personal information is stolen, lost, or accessed by unauthorized persons. (paraphrase)

Alberta *Personal Information Protection Act, 2004, ss. 34.1(1) and 37.1(1)* An organization must without unreasonable delay notify the Commissioner and may be required to notify individuals of any incident involving the loss of or unauthorized access to or disclosure of personal information where a reasonable person would consider there exists a real risk of significant harm to the individuals. (paraphrase)

(Former) Federal Bill C-29 would have modified PIPEDA to create an obligation on the part of organizations to inform the Commissioner of *material* data breaches and to notify individuals of breaches that pose *real risk of significant harm* to individuals affected, in accordance with a scheme that very much resembles the OPC's Voluntary Breach Notification Guidelines (2007).

Sources of Risk

A recent White Paper by Symantec in 2009 entitled "*Anatomy of a Data Breach: Why Breaches Happen and What to do About it*", categorizes the three most common sources of risk for data breaches as follows:

1. well-meaning insiders
2. targeted attacks from outside the organization
3. malicious insiders

Well-meaning (but sometimes negligent) insiders

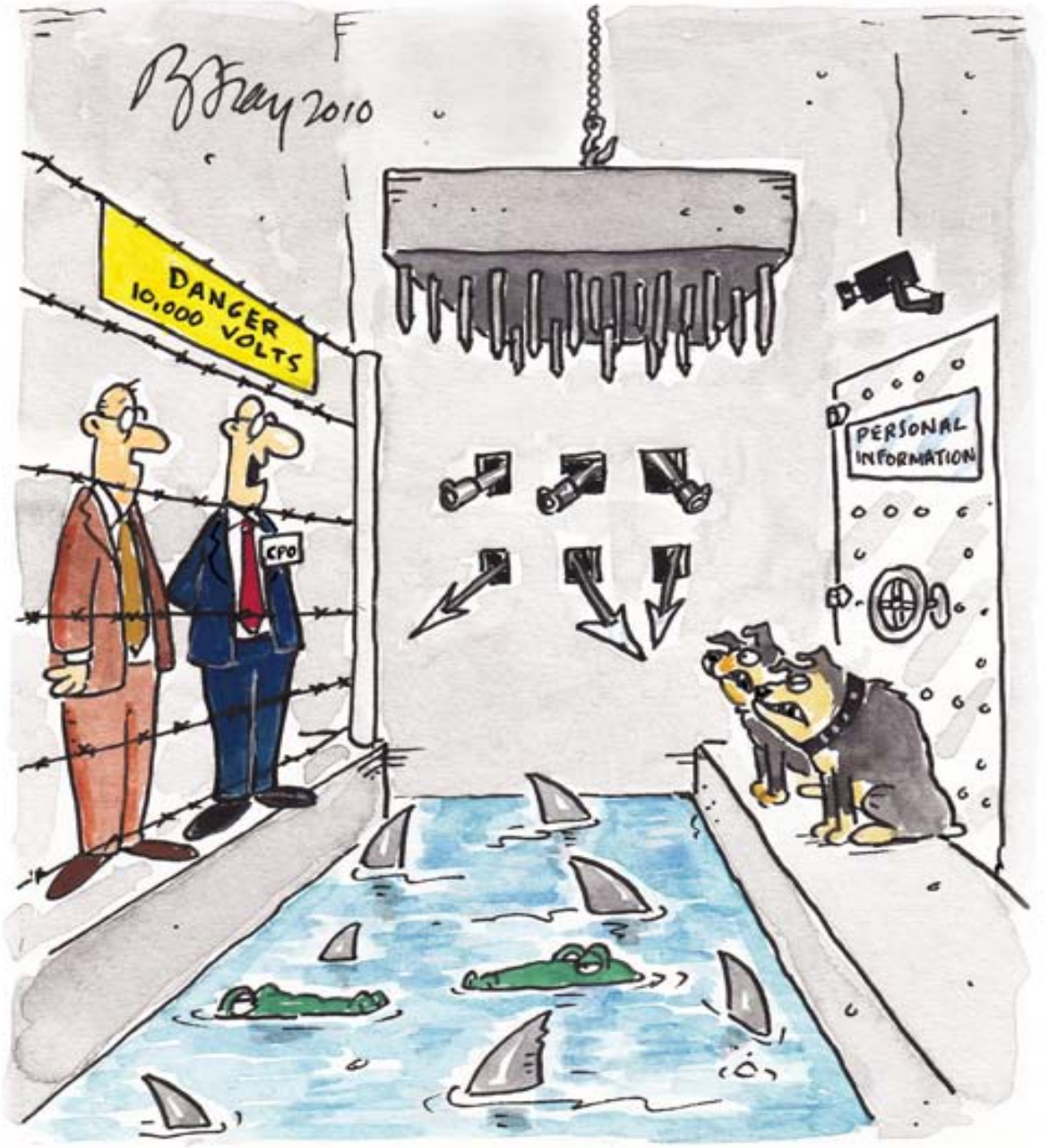
- Data exposed on servers and desktops
- Lost or stolen laptops*
- Email, web mail, and removable devices*
- Third-party data loss incidents*
- Outdated business processes
- (Abandoned records)*

Retention of Files

Targeted Attacks from Outside

- System vulnerabilities & security weaknesses
- Improper credentials (weak identification and authentication procedures)
- Spyware or targeted malware enabling remote access to servers*

Security Safeguards



"I think you'll find our safeguards for protecting your personal information more than adequate!"

Malicious (motivated) Insiders

- White collar crime
- Terminated employees with an axe to grind
- Career advancement with company data*
- Industrial espionage by defectors leaving to join the competition
- (Sad love triangles)*

Direct Costs of a Data Breach

- According to a November 2010 Benchmark Study of the Ponemon Institute (based on 65 respondent healthcare organizations), the economic impact of data breach incidents over a two-year period is approximately $2 million per organization (est. $12 billion total across all hospitals in the U.S.).

- Respondents stated they have inadequate resources (71%), few (if any) appropriately trained personnel (52%) and insufficient policies and procedures in place (69%) to prevent and quickly detect patient data loss.

- Most respondents have little or no confidence in their ability to appropriately secure patient records (58%); but 74% of those that have implemented EHR systems believe that their patient data is more secure.

- 70% say that protecting patient data is not a top priority; 67% have less than two staff dedicated to data protection management; typically, patients are the first to detect privacy breaches at healthcare organizations (41%).

Indirect Costs of a Data Breach

- According to healthcare organizations surveyed in the 2010 Ponemon study, the most negative result of data breach is brand or reputation diminishment (81%); time and productivity loss (80%) and loss of patient goodwill (77%)

- From the perspective of patients, an earlier 2005 Ponemon study found that 58% of respondents who self-reported that they received a notification of a data breach involving their personal data said that the breach event has diminished their trust and confidence in the organization.

- 19% of the same respondents indicated that they have already discontinued or plan to discontinue their relationship with the organization because of the breach, and a further 40% said that they might discontinue their relationship.

Proactive Measures for Breach Mitigating: The "Big" Picture

- Embedding "Privacy by Design" into health information systems upstream as they are being developed

- Inculcating an organizational culture that respects, and is responsive to, legitimate privacy concerns

- Adopting accountability and transparency as guiding principles to enable important work to continue in the public interest and with the public's trust

Conclusions

- Innovation requires system developers to anticipate the broader legal, ethical and societal implications (including respect for personal privacy) and to address them proactively, up front, in the design and development process.

- Innovation calls for innovative approaches. User privacy is not an obstacle to innovation, but rather, a call to develop innovative and creative ways of protecting personal information in step with technological progress and to take leadership in developing best practices for others to follow.

Conclusions

- Privacy is not to be used as an excuse for "secrecy" or a shield for inefficiency or incompetence; it is not the antithesis of transparency or accountability. On the contrary, transparency and accountability are critical conditions for effectively protecting personal data of users, while maintaining their trust in the efficiency of the system and in the performance of its actors.

Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Thank you
Merci

1-800-282-1376

www.priv.gc.ca