Personal Health Data: Patient Consent in Information Age

Dragana Martinovic, Ph.D.\textsuperscript{a}, Victor Ralevich, Ph.D.\textsuperscript{b}, & Milan Petkovic, Ph.D.\textsuperscript{c}

\textsuperscript{a} University of Windsor, Windsor, Ontario, Canada
\textsuperscript{b} Sheridan Institute, Oakville, Ontario, Canada
\textsuperscript{c} Technology University, Eindhoven, Netherlands
Our Research Topics of Interest

- National and international issues of personal (medical) information protection by legislative and technical means.

- Types of patient’s consent related to data release.
  Transfer and use of medical data, including patients’ consent, at the national and international levels.

  Need for legal and semantic consistency in handling and interpreting patients’ consent in cross-
Essential Points of the Work

- Establishing a need for better understanding of technical and legal issues of personal health data management in various geo-political domains.
- Raising awareness of different and unaligned technological and legal approaches in dealing with patients’ privacy preferences.
- Properly addressing the contextual dependencies of patient consent interpretation and implementation.
- Developing recommendations for technical solutions based on the ‘privacy by design’ concept.
Raising an Issue/Data Breaches

A personal data breach is an event in which an individual’s SIN/SSN, driver’s license number, medical record or a financial card number is put at risk – either in electronic or paper format.
Data Breaches Reported in US 2005-2011

Source: Privacy Rights Clearinghouse
Six Healthcare Data Breaches That Might Make Security Pros Sick

Most of the healthcare industry's biggest compromises could have been avoided, experts say

By Ericka Chickowski, Contributing Writer, Darkreading
Aug 13, 2010 | 01:35 PM
URL -

The number of healthcare breaches in 2010 have outpaced other verticals -- including banking and government -- by as much as threefold. While not all of these breaches came via databases, the majority of them could have been prevented through better data access and governance policies -- policies that must be enforced at the database level, experts say.

Healthcare organizations seem particularly prone to problems on the inside of the organization, including malicious theft and unintentional loss of storage devices containing treasure troves of database information. Let's take a look at six of the biggest breaches from recent months -- and the lessons they might teach about data protection
NHS worst for data breaches - Information Commissioner

The NHS has reported the highest number of serious data breaches of any UK organisation since the end of 2007, the Information Commissioner's Office says.

David Smith, deputy commissioner at the ICO told the Infosec security conference the NHS had highlighted 287 breaches to it in the period.

That accounts for more than 30% of the total number reported.

The NHS - the UK’s largest employer with 1.7m staff - is in the process of rolling out digital patient records.

Most of the breaches (113) were the result of stolen data or hardware, followed by 82 cases of lost data or hardware.
Health Net of Connecticut sued for failing to secure patient health records and financial information of nearly 446,000 plan members.

A portable computer disk drive with unencrypted information disappeared from Health Net's Shelton office.
Commissioner Cavoukian expects health sector to encrypt all health information on mobile devices:
Nothing short of this is acceptable

TORONTO – Ontario Information and Privacy Commissioner, Dr. Ann Cavoukian, today directed the province’s health sector not remove from their premises any personal health information on mobile devices – unless this very sensitive information is encrypted, as required in a health order issued in 2007.

This follows the loss last week of a USB key containing the health information of almost 84,000 patients who attended H1N1 flu vaccination clinics in the Durham Region.

This incident is “very distressing,” said the Commissioner, “especially in light of the fact that I directed all Ontario health information custodians not to transport personal health information on laptops or other personal devices unless the information was encrypted.” This direction was implemented in 2007.

Cost of data breaches in the US: According to the Ponemon Institute, it is $6 Billion/year.
Patient Consent
Consumer/Patient Rights

- Fundamental ethical requirements for confidentiality of medical data
- Legislation: The EU Directive 95/46/EC, HIPAA, PHIPA, etc.
Consent Options for Electronic Exchange

1. **No consent**—patients cannot opt out

2. **Opt-out**—health information is included by default, but the patient can opt out completely

3. **Opt-out with exceptions**—same as (2), but the patient can also allow only select data to be included

4. **Opt-in**—default is that no patient health information is included; if patients give consent, their information must be all in

5. **Opt-in with restrictions**—default is that no patient health information is made available, but the patient may allow a subset of select data to be included.
Consent Automated Processing – Some Concerns

- Ambiguities in the consent language and statements
- Proper interpretation of the granular or partial opt-in or opt-out consent in different jurisdictions
- Privacy protection of patients’ data in other jurisdictions (for example: Canada vs. US PATRIOT Act provisions).
The Scope of the Privacy and Consent Issues Internationally

<table>
<thead>
<tr>
<th>Region</th>
<th>Admin. Units</th>
<th>Population</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td>13 provinces</td>
<td>34,559,000</td>
</tr>
<tr>
<td>U.S.A.</td>
<td>50 states</td>
<td>312,047,000</td>
</tr>
<tr>
<td>EU</td>
<td>27 member states</td>
<td>501,064,211</td>
</tr>
<tr>
<td>World</td>
<td>204 sovereign states</td>
<td>6,939,200,000</td>
</tr>
</tbody>
</table>

MIE 2011, Presenter: Victor Ralevich
US HIPPA - Patient Consent

• The patient written consent must be obtained by the covered entities for the use and disclosure of the identifiable health information for the purpose other than they are permitted by the privacy rule.

• Individual has the right to request restriction on the use and disclosure of personal health information, and to request communication to be confidential.

• Each covered entity must provide a notice of its privacy practices to the patient.
Directive 95/46/EC (EU) – Patient Consent

- The consent is any freely given specific and informed indication of data subject’s wishes by which s/he agrees with processing of personal data.
- The EU Directive prescribes that the processing of personal data must be carried out with the consent of the data subject or be necessary under other conditions.
PHIPA (Ontario) – Patient Consent

- Consent to the collection, use or disclosure of personal health information about an individual may be *express* or *implied*.
- The individual may withdraw the consent/has right to access own health records.
- Personal health information may change the custodian if the individual is informed before transferring his/her records or, if that is not reasonably possible, as soon as possible after transferring the records.
Some Questions

- Are there equivalency agreements between countries?
- What are the repercussions of not abiding to the privacy protection legislation (i.e., sanctions, enforcement)?
- How is patient consent treated in various circumstances and what are its legal implications in various domains of use?
- What are prospects for building applicable technologies for automated patient’s consent processing in trans-border circumstances?
Thank you!

Any questions?