Privacy Issues in Consumer Health Applications

Jens H. Weber, PEng, PhD
University of Victoria

jens@acm.org
Have you seen Consumer Health Applications?
What are Consumer Health Applications?

Consumer health [informatics] applications are designed to interact directly with the consumer, with or without the presence of healthcare professionals, and can broadly be divided into community informatics resources—such as health kiosks, community online networks and “cybermedicine” applications that anyone with a home computer can access, —and clinical informatics resources, which are provided to select groups or patients.

The focus of traditional medical informatics is shifting from health professionals to consumers.
Typical CHI Business Models

- Consumers pay
- Employers pay
- Insurers pay
- Providers pay
- Marketers pay
Privacy Threats of CHI

- privilege protection
- subpoenas
- marketing
- breaches

2007 study indicated grave problems: **only 1 in 30 PHR privacy policies require consent prior to disclosing PHI to marketers**

[Altarum 07]
Example Scenario 1

Milt Freudenheim: *And You Thought a Prescription Was Private* NYTimes. August 8, 2009

Over 10 years after buying fertility drugs MCK is still receiving targeted ads in her mail
Can a CHI application vendor make money using PHI for marketing even without disclosing PHI?
Example Scenario 2: Use of PHI for Targeted Marketing

Display targeted ads from pharmaceutical companies on CHI Web pages.

PHI “leaks” to marketer on click-through (cookies, email addresses)
Example Scenario 3: Use of PHI for Targeted Marketing

“Click here to get your blood data analyzed”

What signifies e-consumer consent?
Are CHI applications subject to HIPAA?

*Personal Health Records (PHRs) may be*
ARRA 2009 HITECH Act

- Breach notification for PHRs
- HIPAA extended to Business Associates (BAs) of Covered Entities (CEs)
- PHRs exchanging PHI with CEs must sign associate agreements with CEs
Implications and Discussions

Breach notification rule generally applies to PHRs

PHR’s offered by / or on behalf of CE’s are subject to many of the HIPAA rules (by means of HITECH)

Other PHRs? no - but some choose to comply
Example 1: Yes
Cleveland Clinic Partner Profile

Company

Cleveland Clinic, located in Cleveland, Ohio, is a not-for-profit, multi-specialty academic medical center that integrates clinical and hospital care with research and education. Cleveland Clinic was founded in 1921 with a vision of providing patient care based on the principles of cooperation, compassion and innovation, and has become one of the nation's largest and most respected hospitals. Patients from across America and from more than 80 nations make over three million visits to Cleveland Clinic and its associated health centers every year.

As a recognized leader in health information technology, Cleveland Clinic has implemented a comprehensive electronic medical record infrastructure that connects every caregiver in all its facilities to patients' digital records. When a patient sees multiple physicians, the e-enabled system enhances the ability of the patient's care team to function as a focused, collaborative unit, improving patient safety and quality of care.

"We created a secure connection between Cleveland Clinic's MyChart personal health record service and Google Health because we wanted to help patients everywhere become more fully engaged in their own healthcare activities and decisions," said C. Martin Harris, M.D., Chief Information Officer, Cleveland Clinic. "Connected to services like MyChart, Google Health empowers patients by giving them the ability to make their personal health information available to any physician or other health-related service provider, any time, anywhere they choose."
Illustrating an Ongoing Discussion

MSDN Blogs > Family Health Guy > HIPAA-potamus

HIPAA-potamus

Sean Nolan  3 May 2008 2:12 AM  7

In one of those classic if I had a nickel things ... you have no idea how many times I get asked if HealthVault is "covered" under HIPAA.

The short answer to that question is, very simply, NO.
Fast forward about a year, and "pretty simple" just wasn't good enough for the well-meaning folks in Washington, DC. When they sat down to reform healthcare with the ARRA bill, things got a bit muddled up. Did anything really change that would affect our position? Unfortunately, the answer is really "nobody knows."

Which brings me to the real point here. **We are now prepared to sign a Business Associate Agreement with any covered entity that feels it is an important part of their responsibility under the HIPAA legislation.** We have worked hard to create the text of that BAA, and are committed to being open and transparent about exactly what it contains. In fact, it is posted online for anybody to review here.
Global Reach of Foreign Regulations - An example

Canadian privacy commissioner has jurisdiction to investigate complaints related to the cross-border flow of Canadians’ personal information, as long as there is a real and substantial connection to Canada.

[Ramirez and Marble, 2010]

Recent example: Facebook
[PIPEDA Case Summary #2009-008]

PIPEDA may apply to many PHR offerings
[Williams & Weber, 2010]
Next Challenge: Convergence of CHI and Social Networks

Privacy threats of social networks applications in health care (SNAHCs)

Ultimately, it is your decision to make about how to balance [privacy] risks. [...] The more personal information you share (e.g., photos, location, birthday or other personal information which is optional to add in your profile) on our site, the more risk there is that someone can identify you.
Summary & Conclusions

• Fast growing market for Consumer Health Informatics products and services
• Diverse and strong interest in personal health data
• Privacy policies often insufficient
• Evolving regulatory framework
• Cross-border information flows
References


