Privacy Guidelines Workshop
December 1, 2005

Executive Summary

Prepared by: Mary Lysyk, University of Ottawa.
Khaled El Emam, PhD, University of Ottawa.
Carole Lucock, LLB, LLM, University of Ottawa.
Michael Power, LLB, Gowling Lafleur Henderson LLP.
Donald Willison, PhD, McMaster University.

In an era where information technology (IT) is increasingly taking a prominent role, there is a move by federal, provincial and territorial governments to accelerate the adoption of electronic health records (EHRs) [1-3]. IT facilitates numerous healthcare functions including clinical and population-based health research, as in the development of disease registries or when conducting clinical and genetic database research [4-5].

Privacy has been identified as the issue that may slow and/or impede the progress of EHR implementation [6]. Currently, privacy best practices specific to IT do not exist for the health research community.

The Electronic Health Information and Privacy Workshop was held on December 1, 2005, in Ottawa, Ontario. The workshop is the first step in a broader research program focused on developing electronic health information (EHI) privacy best practices and resource tools to guide researchers, clinicians and research ethics boards (REBs). The workshop brought together privacy, policy and IT experts from across the country and represents the first workshop of its kind in Canada. It served to consolidate key recommendations for developing specific electronic health information best practices that can be applied within the 2005 *CIHR Best Practices for Protecting Privacy in Health Research* guidelines. Like the CIHR Best Practices and owing to the changing nature of IT, the recommendations should be reviewed at least every two years. The principle recommendations that emerged from the workshop are:

Policy Alternatives for the Health Research Community:

1. A model is needed that will integrate the following three policy alternatives into electronic health information privacy best practices for clinical research. The policy alternatives include: 1) Independent prior review of individual projects for privacy confidentiality and security issues; 2) Periodic audit of IT providers; and 3) Provide training and tools (e.g., standardized privacy checklist, e-learning module) for the clinical research community.

2. Privacy accountability frameworks with clear privacy policies should be required for all electronic health information custodians.

3. Threat risk assessments such as privacy impact assessments should be conducted by EHI custodians and IT vendors, as part of a total risk management approach.

4. Lessons learned from practices in e-commerce as well as from other countries utilizing electronic health information systems should be compiled as part of a knowledge transfer mechanism.

Next steps: Future workshops will help guide the development of electronic health information privacy models as well as provide feedback and direction to the development of standardized privacy guidelines (e.g., EHI privacy checklist) and educational resources for the health research community. The need for standardized EHI best practices and educational resources have been identified as priorities for action.

De-identification (anonymization) of Electronic Health Information:

1. Consistent vocabulary or a lexicon of commonly used terms (e.g., anonymization, de-identification, re-identification) should be developed.

2. More research is needed to evaluate re-identification risk of potentially identifying variables in the Canadian context so that guidance can be provided to the health research community (i.e., similar to the HIPAA variable list). Due to the changing nature of IT, this research should continue on an ongoing basis. Specific areas of focus include extending current re-identification risk studies on:

    - Re-linking data across private databases where data sharing is assumed to be on an anonymous basis;

    - Identifying additional sources of data, for example, what information is available commercially through data-brokers (in Canada and the U.S.);

    - Identifying other variables that may pose equal problems to the ones found by Sweeney using date of birth, gender and a partial postal code.

3. Engage other sectors such as justice and the private sector (e-commerce) in this dialogue.

Next steps: El Emam et al. [7] are currently expanding their study on data re-identification risk to include a larger sample size in the province of Ontario and hope to replicate this work in other jurisdictions across the country.

IT Outsourcing:

1. As part of the informed consent process, disclosure is required about security and confidentiality measures including whether data is being outsourced.

2. Establish recognized mandatory standards and selection criteria for IT vendors.

3. Implement formal institutional policies detailing the obligations for data sharing within and between institutions (possible link to an accreditation system).

4. Provide training and best practices for the health research community related to IT outsourcing. Specifically, guidance is needed for REBs about what they need to know and ask.

5. Develop clear contractual agreements (including pro forma contracts), which outline what can be done with outsourced data.

Next steps: IT outsourcing recommendations need to be incorporated into standardized best practice guidelines (e.g., EHI privacy checklist) that would be available to the health research community. A future workshop would serve to further develop, refine and discuss implementation of these strategies.

The workshop outcomes need to be disseminated broadly in order to promote awareness of these issues and generate further reflection and discussion among the health research community, EHI privacy experts and stakeholders, and the broader Canadian public.

References

(1) Commission on the Future of Health Care in Canada, Romanow RJ. Building on values: the future of health care in Canada: final report. Saskatoon: Commission on the Future of Health Care in Canada; 2002.

(2) Health Council of Canada (January 2005). Health Care: Renewal in Canada: Accelerating Change. 2005.

(3) The Standing Committee on Social Affairs, Science & Technology, Kirby MJL. The Health of Canadians-The Federal Role Final Report. 2002.

(4) Gostin LO, Hodge JG. Privacy and Security of Public Health Information. Model State Public Health Privacy Project 1999 February 24 [cited 2005 Dec 12];1-16. Available from: URL: http://www.critpath.org/msphpa/ncshdov.htm

(5) Willison D. Privacy and the secondary use of data for health research: experience in Canada and suggested directions forward. Journal of Health Services Research and Policy 2003;8(1):S1:17-S1:23.

(6) Office of Health and the Information Highway. Toward Electronic Health Records. Health Canada 2001 January [cited 2005 Aug 15];Available from: URL: http//www.hc-sc.gc.ca/ohih-bsi/

(7) El Emam K, Jabbouri S, Sams S, Drouet Y, Power M. Evaluating common de-identification heuristics for personal health information. 2006 J Med Internet Res.