

Safeguarding Privacy: The ICES Experience

Privacy has become an issue larger than celebrity evasion of the paparazzi. While academic health research has observed strict vigilance in the guardianship of health information databases, new legislation faced by all organizations raises the bar. Short of building a moat to secure precious data, research organizations, such as the Institute for Clinical Evaluative Sciences (ICES), are introducing increasingly rigorous policies to keep sensitive information safe while preserving the value of research.

Introduction

The passing of Canada’s federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), in January 2004, and Ontario’s *Personal Health Information Protection Act*, 2004 (Bill 31), in May 2004, prompted the Canadian health services and policy research community to establish standards, policies and procedures for personal health information in administrative databases. Collected for purposes such as physician service claims and drug benefit reimbursement for persons 65 and older, these data are also used for academic health services research. It is costly to perform due diligence on privacy issues and ensure standards are maintained, and most research organizations are struggling to understand privacy legislation and compliance in the first place.

Implementing Privacy Protections

This report describes ICES’ approach to privacy protection, undertaken from November 2000 to December 2003.

Table 1. ICES Privacy Spending November 2000 to December 2003

Activity	Costs	Staff Time Expended (hours)**
1. Preliminary activities	\$ 3,000	~170
2. Confidentiality committee	\$104,991	~1,658
3. Web-based privacy orientation	\$ 9,000	~100
4. ICES/CCO PIA*	\$ 8,760	—
5. Internal PC audit	—	~ 304
6. Encryption software	\$ 3,178	~20
7. Educational conferences	\$ 6,235	—
8. Legal fees†	\$ —	—
9. Miscellaneous costs	\$ 4,827	—
TOTAL	\$139,991	1,658 costed hours (.85 FTE) 594 uncosted hours (.30 FTE)

*PIA = Privacy Impact Assessment. **Derived from staff time-logging system. †See Table 3

Results

1. Preliminary Activities

With expert consultation, prioritized tasks were planned for implementation between 2001 and 2004. An ICES staff

member was assigned to work with the consultant to develop a privacy code based on a template. Refinements were made by e-mail and teleconference.

2. Employee Committee

A 12-member confidentiality committee with multi-departmental representation worked on privacy and data security issues and improvements to the draft privacy code. Time/cost estimates were derived from ICES’ time management database. Activities included items (a) to (h) from Table 2, with associated time equaling .85 of one full-time equivalent.

Table 2. Core Privacy-Related Activities

- a) Draft privacy code and executive summary;
- b) Produce public information brochure;
- c) Web-post privacy code/summary/public brochure;
- d) Write, review and edit policies and practices (data access; building/office access and security; staff confidentiality agreements; data confidentiality and security; ethics review process; shredding and password policies; breach, data destruction and disaster recovery plans; staff orientation);
- e) Develop flow charts for data movement and security;
- f) Bi-weekly meetings of confidentiality committee;
- g) Create handbooks (1) staff (2) contract workers/abstractors;
- h) Organize privacy/data security library and manuals;
- i) Perform PC audit;
- j) PIA by privacy consultant;
- k) Design Web-based staff orientation;
- l) Professional consulting and legal counsel.

3. Web-Based Privacy Orientation

To standardize training and reduce the burden of conducting 244 individual 30 to 60 minute sessions, a senior student programmer was hired to develop a Web-based orientation. The program was written in ZOPE (freeware) and is designed for easy editing and sharing with other research organizations. In addition to \$9,000 in programmer fees, the privacy officer, a staff member with privacy experience, and a systems manager invested approximately 100 hours.

4. Privacy Impact Assessment (PIA)

An independent privacy consultant performed an assessment of systems, policies and procedures in August 2003, as part of an approval process for transferring important registry data to ICES. Though most costs were covered by the other agency, ICES assumed some preparation costs, including a full-day meeting of senior personnel with the consultant.

5. Internal PC Audit

The privacy officer, with assistance from the systems group, audited almost 80% of individual PCs (103) linked to ICES’ local area network for compliance with policies and procedures. Conducted on a part-time basis over eight months, the half-hour sessions in actuality ranged from 10 to 30 minutes, and 10% exceeded the allotted time. Some staff indepen-

dently accessed the search algorithm and methodology to check their own computers and address any problems. Total time invested was 304 hours, including systems preparation, audit committee planning, audit sessions, report creation and an estimate of undocumented time.

6. Encryption Software

Concern about protection of chart abstraction data in the field in the event of laptop theft or service requirements and protection of sensitive internal personnel data, prompted selection of versatile and easy-to-use encryption software that can sit on different platforms used at ICES.

7. Educational Conferences and Meetings

The particulars of data security and privacy standards are evolving rapidly. Investment in educational meetings and conferences will help increase knowledge to increase capacity for cross-coverage and monitoring organizational performance.

8. Legal Fees

In addition to the costs outlined in Table 1, ICES incurred significant legal costs associated with privacy protections.

ICES research in conjunction with stakeholder agencies requires complex agreements for management of data collection, use and disclosure, custodianship and clarification of intellectual property (IP). As such, additional fees for expertise in law, privacy and IP specific to the Bill between January 1 – October 1, 2004, were in the range of \$50,000.

April 1, 1999 to Dec. 31, 2003	\$ 8,929
Jan. 1, 2004 to Oct. 1, 2004 (Bill 31 period)	~\$50,000
Total	\$58,929

9. Miscellaneous Costs

Other privacy-related costs incurred over the four fiscal years include office supplies, catering, postage, long distance calls, photocopying and books.

Conclusion

In applications for infrastructure funding and other grant proposals, it is important for researchers and their organizations to be able to factor in the costs of implementing privacy protections and maintaining required standards. An even bigger issue is the challenge in understanding the obligations of provincial legislation, PIPEDA and the tangle of privacy principles found in Schedule I (CSA Standards: the Ten Guiding Principles). In addition, it is difficult to find privacy-knowledgeable staff and qualified individuals to do privacy impact assessments, and it is expensive to train employees, implement policies and procedures, and maintain educational



Transforming health care organizations through a focus on strategy, people, work and performance:

- Planning
- Operational Improvement
- Organizational Effectiveness
- Human Resources Management
- Reward Programs

Contact:
Mark Hundert
National Director
Tel: (416) 868-1371
Fax: (416) 868-0362

programs. Finally, time measures shown here are conservatively underestimated, as data is reliant on time input (or not) by staff, and by unlogged time contributed by the Board of Directors for policy review.

To maximize best practices, a national workshop series conducted in 2003/04 on *Harmonizing Research and Privacy: Standards for a Collaborative Future*, sponsored by the Canadian Institutes for Health Research, encouraged researchers to share privacy tools. Practices, policies and procedures from participant organizations were collated by sponsoring agencies (ICES and the Manitoba Centre for Health Policy). The resulting CD template toolkit has helped save some organizations time and expense while providing a standardized approach to privacy that can be tailored to the specific needs and legislative requirements of other organizations. For more information, contact info@ices.on.ca.

About the Authors

At the Institute for Clinical and Evaluative Sciences, **Pamela M. Slaughter** is Privacy Officer; **Carolynne Varney** is Senior Communications Officer; **Kevin Leman** is Director, Finance; and **Peggy McGill** is VP Corporate Services.