



Information and Privacy
Commissioner of Ontario
Commissaire à l'information
et à la protection de la vie privée de l'Ontario

October 31, 2011

VIA ELECTRONIC AND REGULAR MAIL

Dr. David A. Henry, President and CEO
Institute for Clinical Evaluative Sciences
G Wing, 2075 Bayview Avenue
Toronto, Ontario
M4N 3M5

Dear Dr. Henry:

**RE: Review of the Report on the Practices and Procedures of the Institute for
Clinical Evaluative Sciences**

Pursuant to subsection 45(4) of the *Personal Health Information Protection Act, 2004* ("the Act"), my office is responsible for reviewing the practices and procedures implemented by each prescribed entity to protect the privacy of individuals whose personal health information it receives, and to protect the confidentiality of that information, every three years.

Given the practices and procedures of the Institute for Clinical Evaluative Sciences (ICES), a prescribed entity within the meaning of the *Act*, were last approved on October 31, 2008, my office was again required to review these practices and procedures and advise whether they continue to meet the requirements of the *Act* on or before October 30, 2011.

In accordance with the new process as set out in the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* ("the Manual"), ICES, as a prescribed entity which was seeking the continued approval of its practices and procedures, submitted a detailed written report and sworn affidavit to my office. These documents were to conform to the requirements set out in the *Manual*.

My office has now completed its review of your report and affidavit. Based on this review, I am satisfied that ICES continues to have in place practices and procedures that sufficiently protect the privacy of individuals whose personal health information it receives, that sufficiently maintain the confidentiality of that information and that continue to meet the requirements of the *Act*.

Accordingly, effective October 31, 2011, I am pleased to advise that the practices and procedures of ICES continue to be approved for a further three-year period.

Attached is an Appendix containing recommendations to further enhance the practices and procedures of ICES, which must be implemented prior to the next legislated review.

.../2



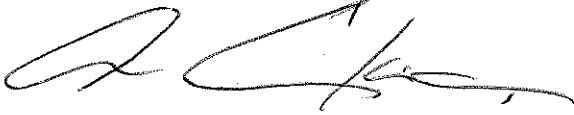
Legal Services Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Services juridiques
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Télééc: 416-325-9186
TTY: 416-325-7539
www.ipc.on.ca

I would like to extend my gratitude to you and your staff for the cooperation provided during the course of the review, including the diligence and timeliness in submitting the requested documentation, in responding to requests by my office for further information and in making the amendments requested.

Sincerely yours,

A handwritten signature in black ink, appearing to read 'Ann Cavoukian', with a stylized, flowing script.

Ann Cavoukian, Ph.D.
Commissioner

cc: Pam Slaughter, Chief Privacy Officer

Appendix

It is recommended that ICES address the recommendations listed below, in accordance with the requirements of the *Manual* prior to the next review of its practices and procedures:

1. Create and maintain logs to track and enable the reporting of the following information:

- (a) The dates that the privacy policies and procedures were reviewed by ICES since the prior review of the Information and Privacy Commissioner of Ontario.
- (b) Whether amendments were made to existing privacy policies and procedures as a result of the review, and if so, a list of the amended privacy policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.
- (c) Whether new privacy policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.
- (d) The date that each amended and newly developed privacy policy and procedure was communicated to agents and, for each amended and newly developed privacy policy and procedure communicated to agents, the nature of the communication.
- (e) Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.

2. Create and maintain logs to enable the tracking and reporting of the following information:

- (a) The dates of audits of agents granted approval to access and use personal health information since the prior review by the Information and Privacy Commissioner of Ontario and for each audit conducted:
 - A brief description of each recommendation made,
 - The date each recommendation was addressed or is proposed to be addressed, and
 - The manner in which each recommendation was addressed or is proposed to be addressed.
- (b) The number and a list of all other privacy audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit:
 - A description of the nature and type of audit conducted,
 - The date of completion of the audit,
 - A brief description of each recommendation made,
 - The date each recommendation was addressed or is proposed to be addressed, and

- The manner in which each recommendation was addressed or is proposed to be addressed.
3. It appears, from the information provided, that the numbers of notifications of privacy breaches or suspected privacy breaches received by ICES is recorded. Other required information may be maintained as well, however, it was not clear from the information provided. Accordingly, ICES should ensure that it maintains logs to enable the tracking and reporting of the following information:
- (a) With respect to each privacy breach or suspected privacy breach:
- The date that the notification was received,
 - The extent of the privacy breach or suspected privacy breach,
 - Whether it was internal or external,
 - The nature and extent of personal health information at issue,
 - The date that senior management was notified,
 - The containment measures implemented,
 - The date(s) that the containment measures were implemented,
 - The date(s) that notification was provided to the health information custodians or any other organizations,
 - The date that the investigation was commenced,
 - The date that the investigation was completed,
 - A brief description of each recommendation made,
 - The date each recommendation was addressed or is proposed to be addressed, and
 - The manner in which each recommendation was addressed or is proposed to be addressed
4. Create and maintain logs to track and enable the reporting of the following information:
- (a) The dates that the security policies and procedures were reviewed by ICES since the prior review of the Information and Privacy Commissioner of Ontario.
- (b) Whether amendments were made to existing security policies and procedures as a result of the review and, if so, a list of the amended security policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.

- (c) Whether new security policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.
 - (d) The dates that each amended and newly developed security policy and procedure was communicated to agents and, for each amended and newly developed security policy and procedure communicated to agents, the nature of the communication.
 - (e) Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.
5. Create and maintain logs to track and enable the reporting of the following information:
- (a) The dates of audits of agents granted approved to access the premises and locations within the premises where records of personal health information are retained since the prior review by the Information and Privacy Commissioner and for each audit:
 - A brief description of each recommendation made,
 - The date each recommendation was addressed or is proposed to be addressed, and
 - The manner in which each recommendation was addressed or is proposed to be addressed.
6. Create and maintain logs to track and enable the reporting of the following information:
- (a) The dates of the review of system control and audit logs since the prior review by the Information and Privacy Commissioner of Ontario and a general description of the findings, if any, arising from the review of system control and audit logs.
 - (b) The number and a list of security audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit:
 - A description of the nature and type of audit conducted,
 - The date of completion of the audit,
 - A brief description of each recommendation made,
 - The date that each recommendation was addressed or is proposed to be addressed, and
 - The manner in which each recommendation was addressed or is expected to be addressed.
7. Create and maintain logs to track and enable the reporting of the following information:

- (a) The dates and number of communications to agents by ICES in relation to privacy since the prior review by the Information and Privacy Commissioner of Ontario and a brief description of each communication.
8. Create and maintain logs to track and enable the reporting of the following information:
 - (a) The number of agents who have attended and who have not attended ongoing security training each year since the prior review by the Information and Privacy Commissioner of Ontario.
 - (b) The dates and number of communications to agents by ICES to agents in relation to information security since the prior review by the Information and Privacy Commissioner of Ontario.
 9. Create and maintain logs to track and enable the required reporting of the following information:
 - (a) The dates that the corporate risk register was reviewed by ICES since the prior review by the Information and Privacy Commissioner of Ontario.
 - (b) Whether amendments were made to the corporate risk register as a result of the review, and if so, a brief description of the amendments made.
 10. Create and implement a business continuity and disaster recovery plan, which accords with the requirements of the *Manual* and create and maintain logs to enable the tracking and reporting of the following:
 - (a) The dates that the business continuity and disaster recovery plan was tested since the prior review by the Information and Privacy Commissioner of Ontario.
 - (b) Whether amendments were made to the business continuity and disaster recovery plan as a result of the testing, and if so, a brief description of the amendments made.
 11. Amend the agreement between ICES and the third-party service provider, retained to securely destroy records of personal health information, to ensure consistency with Order HO-001 and with the provisions set out in *Fact Sheet 10: Secure Destruction of Personal Information*, issued by the IPC.
 12. Develop and implement a policy and procedures for ongoing review of privacy and security policies, procedures and practices, which accords with the requirements of the *Manual*.
 13. Develop and implement a policy and procedures for statements of purpose for data holdings containing personal health information, which accords with the requirements of the *Manual*.
 14. Develop and implement a policy and procedures for limiting agent access to and use of personal health information, which accords with the requirements of the *Manual*.
 15. Develop and implement a policy and procedures regarding Privacy Impact Assessments, which accords with the requirements of the *Manual*.