Information
and Privacy
Commissioner/
Ontario

Report of the Information & Privacy Commissioner/Ontario

Review of the INSCYTE (Information System for Cytology etc.) Corporation in respect of CytoBase:

A Prescribed Person under the *Personal Health Information Protection Act*

Ann Cavoukian, Ph.D.
Commissioner
October 2005

Review of the INSCYTE (Information System for Cytology etc.) Corporation in respect of CytoBase:
A Prescribed Person under the *Personal Health Information Protection Act*

The *Personal Health Information Protection Act, 2004* (*PHIPA*) came into effect on November 1, 2004. The Information and Privacy Commissioner of Ontario (IPC) has been designated as the oversight body responsible for ensuring compliance with *PHIPA*. *PHIPA* establishes rules for the collection, use and disclosure of personal health information by health information custodians that protect the confidentiality and the privacy of individuals with respect to that personal health information. In particular, *PHIPA* provides that health information custodians may only collect, use and disclose personal health information with the consent of the individual to whom the personal health information relates or as permitted or required by *PHIPA*.

Responsibilities of Prescribed Persons

Section 39(1)(c) of *PHIPA* permits health information custodians to disclose personal health information without consent to certain prescribed persons who compile or maintain registries for purposes of facilitating or improving the provision of health care or that relate to the storage or donation of body parts or bodily substances ("prescribed persons").

Section 13(2) of Regulation 329/04 to *PHIPA* requires each prescribed person to have in place practices and procedures to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of the information. Section 13(2) further requires each prescribed person to ensure that these practices and procedures are approved by the IPC prior to November, 1, 2005, in order for health information custodians to be able to disclose personal health information to the prescribed person without consent and for the prescribed person to:

- be able to collect personal health information from health information custodians;
- use personal health information as if it were a health information custodian for purposes of section 37(1)(j) or section 37(3) of *PHIPA*; and
- disclose personal health information as if it were a health information custodian for purposes of sections 44, 45 and 47 of *PHIPA*.

Further, section 13(3) requires prescribed persons to make publicly available a plain language description of the functions of the registry, including a summary of the practices and procedures to protect the privacy of individuals whose personal information it receives and to maintain the confidentiality of that information.

Mandate of the IPC with Respect to Prescribed Persons

Prescribed persons must ensure that their practices and procedures to protect the privacy of individuals whose personal health information they receive and to maintain the confidentiality of that information are reviewed and approved by the IPC prior to November 1, 2005.

Review Process

The IPC met with all of the prescribed persons to outline the process that would be followed by the IPC for the review of these practices and procedures. The process was to include a review of documentation relating to the practices and procedures of the prescribed person to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of that information, as well as a visit to the primary site where personal health information was held by the prescribed person. The IPC provided the prescribed persons with a preliminary checklist of privacy and security measures that the IPC would be looking for during the course of its review. The checklist included the following:

Human Resources

- Confidentiality agreements
- Disciplinary procedures for violations
- Clearly defined roles and responsibilities
- Appointed contact persons for privacy and security
- Ongoing education and training program for all staff, employees, affiliates, volunteers, etc. on security and privacy policies and procedures
- Third party agreements (with health information custodians, researchers, etc.)

Privacy

- Privacy policies and procedures that describe how the organization adheres to each fair information practice
- Privacy brochure – available upon request to the public
- Privacy Impact Assessments – for programs/database holdings
- Internal/external privacy audits
- Privacy crisis management protocols
- Data linkage protocols

- Procedures for de-identifying data
- Retention schedules and disposal procedures
- Inventory of all data holdings of personal health information
- Protocol for reviewing proposals in terms of their privacy impacts
- Mechanism for reviewing and updating privacy policies and procedures

Security

- Comprehensive security program including physical, technical and administrative measures
- Access control procedures – authentication and authorization
- Perimeter control
- Electronic access control
- Secure transfer procedures
- Audit trails
- Internal/external security audits
- Disaster Recovery Plan
- Mechanism for reviewing and updating security policies and procedures

The prescribed persons were informed that they were required to implement privacy and security measures and safeguards commensurate with the nature of the work undertaken by the prescribed person, the amount and sensitivity (e.g., level of identifiability) of the information in the custody and control of the prescribed person, and the number and nature of the individuals who have access to personal health information. The scope of the review was to include practices and procedures relating to personal health information included in the registry associated with the prescribed person under section 13(1) of Regulation 329/04.

A site visit was to be scheduled within one month of the IPCs receiving the documentation from the prescribed person. The purpose of the site visit was to provide the prescribed person with an opportunity to provide additional information to the IPC and to clarify their practices and procedures, and to provide the IPC with an opportunity to:

- review the physical, technological and administrative security measures implemented;
- ask questions about the documentation provided; and
- discuss privacy and security matters with appropriate staff of the prescribed person.

Following the document review and site visit, each prescribed person was to be informed of any action that it needed to take prior to having its practices and procedures approved by the IPC. Once all necessary action had been taken or if no action was necessary, the IPC would prepare a draft report that would be submitted to the prescribed person for review and comment. If the IPC was satisfied that the prescribed person had implemented practices and procedures that were sufficient to protect the privacy and confidentiality of personal health information, a letter of approval would be issued prior to November 1, 2005.

Description of the Prescribed Person

INSCYTE Corporation (INSCYTE) is a prescribed person who compiles or maintains a registry under section 39 of *PHIPA*. This registry is called CytoBase.

INSCYTE, a not-for-profit corporation with a Board of Directors, is a partnership of medical laboratories and Cancer Care Ontario. It was founded in 1995 to manage and operate a centralized database (CytoBase) of cervical cancer screening test results in order to assist with the ongoing diagnosis, treatment and follow up of patients. CytoBase also maintains a tracking and physician notification system to ensure individual women are appropriately screened and followed-up and is a source of epidemiological and screening program management information. INSCYTE is funded by Cancer Care Ontario.

INSCYTE collects personal health information through its member laboratories that receive and analyze specimens from individuals. Information is disclosed to member laboratories to permit the analysis of specimens in the context of previous results compiled and retained by CytoBase. Personal health information is also disclosed to registered clinicians, other health care providers, and to Cancer Care Ontario.

The CytoBase system was designed, developed and implemented by Artificial Intelligence in Medicine Incorporated (AIM). AIM is responsible for the day-to-day operation of CytoBase.

Review of the Prescribed Person

Documents Reviewed

INSCYTE provided the IPC with a binder of documents on August 19, 2005, including:

Organizational Materials

- Protocols and Procedures governing the collection, use, disclosure and protection of personal health information, Draft – August 5, 2005 and Final Draft Sept. 20, 2005
- Privacy Delegation Chart and Flow of Accountability

- Source list of Personal Health Information
- Points of Personal Health Information Disclosure
- Inventory of Data Holdings
- Provider Application, CytoBase for Clinicians
- Delegate Application, CytoBase for Clinicians
- Pathologist Application, CytoBase for Clinicians
- Data Sharing Agreement
- Confidentiality & Non-Disclosure Agreement
- Request for Individual Access to Personal Health Information
- Compliance Challenge Form
- Request for Change of Database Information
- Artificial Intelligence in Medicine Inc. (AIM) Agreement for Information System Management Services with appendices (list of AIM staff, list of licensed facilities, CytoBase Operations, Maintenance, Administration and Upgrade Fees, Software and Hardware Supported).
- AIM Staff Authorized to Access Personal Health Information

Security Materials

- CytoBase Security Controls and Performance, Revision 3, August, 2005
- Technical Report, Security Protocols: Encryption of Data and Authentication of Sender/Receiver

Public Privacy Statements/Brochures

- INSCYTE Corporation Privacy Code Draft July 8, 2005 & Final Draft Sept. 20, 2005
- Privacy Brochure (revised Aug 5, 2005)

Site Visit

IPC representatives conducted a site visit at INSCYTE on September 15, 2005.

IPC representatives met with the President of INSCYTE, Board Member and CEO of AIM Inc. and the Privacy Officer, VP Engineering, AIM Inc. Discussions focused on the following topics:

- CytoBase Operations
- Privacy & Security Controls
- Privacy Policies Procedures & Awareness
- Privacy Binder materials

Findings of the Review

Human resources

INSCYTE has clearly defined roles for privacy and security. The President is responsible for ensuring that INSCYTE's activities are consistent with its privacy policies and procedures. The President is accountable to the Board of Directors and has appointed a Privacy Officer who oversees the organization's compliance with the privacy policies and procedures on a day-to-day basis.

All employees of INSCYTE and its agents have undergone privacy awareness training. All new employees are provided with a copy of INSCYTE's Privacy Code and Protocols and Procedures documents and must undergo privacy awareness training, regardless of whether the individual will have access to personal health information. In addition, INSCYTE conducts periodic staff meetings and provides documentation to promote privacy and security awareness and to promote best practices with respect to safeguarding personal health information.

Every employee of INSCYTE or it agents that uses personal health information is required to sign a Confidentiality and Non-Disclosure Agreement. By signing this agreement, individuals acknowledge that they have read, understood and agree to abide by INSCYTE's Privacy Code and its Procedures and Protocols. Individuals also acknowledge that privacy violations will result in disciplinary action including termination of employment or contract. These agreements are renewed on an annual basis.

The sharing of personal health information among INSCYTE and its member organizations is covered by data sharing agreements. In addition, applicants who wish to have access to the CytoBase system must agree to use the information only for the intended purposes and to treat the information as confidential. All delegated users of the CytoBase system must be registered and sign a confidentiality agreement. Registrations are renewed on an annual basis. The disclosure of personal health information to Cancer Care Ontario is covered by a data sharing agreement. There is also a service agreement between AIM and INSCYTE.

It is our understanding that, when the agreements between INSCYTE, its participating laboratories, Cancer Care Ontario and AIM come up for renewal, the wording regarding privacy and security will be revised to accord with the language and requirements of *PHIPA*. With respect to the agreement with Cancer Care Ontario, this agreement should specifically state that the disclosure of personal health information is being made primarily for the purposes of section 45 of *PHIPA* and that the personal health information may only be used and disclosed by Cancer Care Ontario for purposes permitted under *PHIPA*.

When these agreements are revised and renewed, copies should be forwarded to the IPC.

Privacy

INSCYTE has a comprehensive privacy policy. This policy describes how INSCYTE adheres to each of the 10 fair information practices. The privacy policy is augmented by a Protocols and Procedure document which sets out detailed information on how each fair information practice is implemented. The privacy policy is available on INSCYTE's website, along with its Privacy Brochure, Frequently Asked Questions, and contact information for the Privacy Officer.

INSCYTE does not have a protocol for disclosing personal health information for research purposes and it is our understanding that INSCYTE does not disclose personal health information to any third party for research purposes. If, at some point in the future, INSCYTE decides to use or disclose personal health information without consent for research purposes, a policy that incorporates all of the relevant requirements of section 44 of *PHIPA* should be developed and implemented and forwarded to the IPC for review and comment.

Since the CytoBase system is primarily used to provide health care services to individuals, personal health information is not routinely de-identified before it is used. However, INSCYTE does have a formal policy for de-identifying data that applies to the disclosure of person level data where there is no legal authority for the disclosure of personal health information.

INSCYTE has a policy for dealing with privacy breaches. This policy focuses on containing the breach and taking corrective action to ensure that a similar breach does not occur in the future. All breaches are documented and reported to the Privacy Officer, the President and the Board of Directors. In the event of a significant privacy breach, the offending individual's employer or licensing authority is notified and CytoBase system access privileges are revoked. Where appropriate, individuals are notified if their privacy has been breached.

INSCYTE has a protocol in place for linking data within the CytoBase system. Data is linked to provide historical screening information about individual patients. Linkages that take place with external databases require a data sharing agreement.

INSCYTE also has in place a protocol for dealing with privacy complaints. Complaints are sent to the President who refers the complaint to the Privacy Officer. The Privacy Officer is responsible for notifying appropriate parties and attempting to resolve the complaint.

In terms of retention of personal health information, it is our understanding that the intent is to retain all data for the duration of the registry. Nevertheless, INSCYTE has developed and implemented a formal policy for the destruction of data on various media.

Security

A summary review of INSCYTE's information security policies, procedures and other documentation was undertaken, along with an inspection of the physical premises and interviews with relevant IT staff. On the basis of our visit, examination, and observations we found no evidence of major security risks, threats or breaches. We are therefore broadly satisfied that INSCYTE's information security measures are adequate for the purposes of protecting the privacy of personal health information held.

INSCYTE has a security program that incorporates physical, technical and administrative security measures. Although the office where CytoBase is housed is open to the public during normal business hours, the data centre is locked at all times and access is controlled with a pass card lock. Personal health information may only be accessed from secure locations in the office. Outside of normal business hours, the building is locked and protected with an alarm, a security guard and exterior video surveillance cameras.

In terms of information system security, the local area network security over which personal health information is accessed is administered centrally and logically separated from any other network to prevent personal health information from being mixed with other business information. Workstations are set to shutdown after ten minutes of inactivity. All network passwords have a mandatory expiry.

Where the network is accessed from an external unsecured network, such as the Internet, a commercial grade firewall system that controls and audits the access and a commercial grade intrusion detection system that monitors access and alerts system operators to possible attempts at intrusion are required. In addition, data that is transmitted over unsecured networks, such as the Internet, must be encrypted.

In terms of electronic access controls for the CytoBase system, every authorized user of the system is assigned a separate account and password. Application level passwords have a mandatory expiry. Clinicians must re-register to use the system on an annual basis. In terms of audit logs, access and transactions are logged by user account and monitored on a regular basis. Data transmissions to and from the member laboratories are also logged and monitored.

Whenever possible, personal health information that is transmitted via CDs or other electronic media is password protected. Printed personal health information that must be transported is either hand delivered by the staff of INSCYTE or its agents or by bonded courier or registered mail.

A disaster recovery plan has been developed and implemented.

Although INSCYTE has implemented a wide range of security measures, the IPC recognizes that information security requires ongoing vigilance and a commitment to continuous improvement. Given the volume and sensitivity of the personal data stores held and used by INSCYTE and its agents, we would be more comforted by the adoption of a more comprehensive and systemic information security management program.

In this light, then, we encourage INSCYTE to carry out (preferably by an independent party) a comprehensive, organization-wide threat and risk assessment (TRA). Such a TRA would help identify all risks, both external and internal, and provide a strong basis for prioritizing those risks and developing an action plan to mitigate them. Recurring TRAs are also valuable for measuring progress and ensuring continued improvement.

Summary of Recommendations

Major Recommendations

Based on the review of documentation and the site visit, there are no major recommendations that require rectification or resolution by INSCYTE in respect of CytoBase prior to November 1, 2005.

Other Recommendations

Based on the review of documentation and the site visit, the IPC is making the following recommendations that INSCYTE in respect of CytoBase is not required to act upon/resolve prior to November 1, 2005:

1. Amend the agreements between INSCYTE, its participating laboratories, Cancer Care Ontario and AIM to accord with the language and requirements of *PHIPA*.

2. Once the above-mentioned agreements have been revised and renewed, copies should be forwarded to the IPC.

3. Should INSCYTE decide to use or disclose personal health information without consent for research purposes, a policy that incorporates all of the relevant requirements of section 44 of *PHIPA* should be developed and implemented and forwarded to the IPC for review and comment.

4. Conduct regular comprehensive threat and risk assessments, with emphasis on both internal and external threats to security.

Statement of IPC Approval of Practices and Procedures

The IPC is satisfied that INSCYTE in respect of CytoBase has in place practices and procedures that sufficiently protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. Accordingly, effective October 31, 2005, the practices and procedures of INSCYTE in respect of CytoBase have been approved by the IPC.