Information
and Privacy
Commissioner of
Ontario

Report of the Information & Privacy Commissioner/Ontario

Review of the INSCYTE Corporation in respect of CytoBase:

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

Ann Cavoukian, Ph.D.
Commissioner
October 2008

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Three-Year Review of the INSCYTE Corporation in respect of CytoBase:
A Prescribed Person under the *Personal Health Information Protection Act*

The *Personal Health Information Protection Act, 2004* ("the *Act*") is a consent-based statute, meaning that persons or organizations in the health sector defined as "health information custodians"[1] may only collect, use and disclose personal health information with the consent of the individual to whom the personal health information relates, subject to limited exceptions where the *Act* permits or requires the collection, use or disclosure to be made without consent.

One such disclosure that is permitted without consent is the disclosure of personal health information to prescribed persons that compile or maintain registries of personal health information 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 pursuant to subsection 39(1)(c) of the *Act*.

Statutory Provisions Relating to the Disclosure to Prescribed Persons

Subsection 39(1)(c) of the *Act* permits health information custodians to disclose personal health information, without consent, to a prescribed person who compiles or maintains a registry of personal health information for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances. The following persons have been prescribed for purposes of subsection 39(1)(c) of the *Act*:

- Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network;
- Cancer Care Ontario in respect of the Colorectal Cancer Screening Registry;
- Cardiac Care Network of Ontario in respect of its registry of cardiac services;
- INSCYTE Corporation in respect of CytoBase; and
- Hamilton Health Sciences Corporation in respect of Critical Care Information System.

In order for a health information custodian to be permitted to disclose personal health information to a prescribed person without consent, the prescribed person must have in place practices and procedures approved by the Information and Privacy Commissioner/Ontario ("IPC") to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information pursuant to subsection 13(2) of Regulation 329/04 to the *Act*.

1 Persons or organizations described in subsection 3(1) of the *Act* that have custody or control of personal health information as a result of or in connection with performing the powers, duties or work of the person or organization.

These practices and procedures must also be reviewed by the IPC every three years from the date of their initial approval, pursuant to subsection 13(2) of Regulation 329/04 to the *Act*, in order for a health information custodian to be able to continue to disclose personal health information to a prescribed person without consent, and in order for a prescribed person to be able to continue to collect, use and disclose personal health information without consent as permitted by the *Act*.

Initial Review of the Practices and Procedures of the Prescribed Persons

In 2005, the IPC reviewed the practices and procedures implemented by the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network, the Cardiac Care Network of Ontario in respect of its registry of cardiac services and INSCYTE Corporation in respect of CytoBase. Following this review, the IPC approved the practices and procedures implemented by these prescribed persons to protect the privacy of individuals whose personal health information they receive and to maintain the confidentiality of that information, effective October 31, 2005.

While the IPC was satisfied that these prescribed persons had practices and procedures in place that sufficiently protected the privacy of individuals whose personal health information they received and sufficiently protected the confidentiality of that information, the IPC did make certain recommendations to further enhance these practices and procedures. The recommendations made during the initial review of INSCYTE Corporation in respect of CytoBase, which were the subject of an earlier report of the IPC and which are set out in Appendix "A" to this report, have all since been addressed by INSCYTE Corporation.

Three-Year Review of the Practices and Procedures of the Prescribed Persons

Subsection 13(2) of Regulation 329/04 to the *Act* requires the IPC to review the practices and procedures implemented by each prescribed person every three years from the date that they were initially approved by the IPC. Given that the practices and procedures of the Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network, the Cardiac Care Network of Ontario in respect of its registry of cardiac services and INSCYTE Corporation in respect of CytoBase were all approved on October 31, 2005, the IPC was again required to review the practices and procedures implemented by each of these prescribed persons on or before October 31, 2008.

Process Followed for the Three-Year Review

By letter dated January 28, 2008, the Assistant Commissioner for Personal Health Information requested the Canadian Stroke Network in respect of the Registry of the Canadian Stroke

Network, the Cardiac Care Network of Ontario in respect of its registry of cardiac services and INSCYTE Corporation in respect of CytoBase to forward certain documentation to the IPC, set out in Appendix "B" to this report, to enable the IPC to commence its review of the practices and procedures implemented to protect the privacy of individuals whose personal health information is received and to protect the confidentiality of that information.

Upon receipt, the requested documentation was reviewed and additional documentation and necessary clarifications were requested. INSCYTE Corporation in respect of CytoBase submitted the requested documentation on June 24, 2008 and additional documentation on July 31, 2008.

Once the additional documentation and necessary clarifications were received, an on-site meeting was held to discuss the practices and procedures implemented by the prescribed person and to provide the IPC with an opportunity to ask questions arising from the documentation. The on-site meeting with the INSCYTE Corporation in respect of CytoBase was held on August 6, 2008.

Following the on-site meeting, each prescribed person was informed of the action that it was required to take prior to the continued approval of its practices and procedures. Once all necessary action was taken, the IPC prepared a draft report that was submitted to each prescribed person for review and comment prior to the report being posted on the IPC website.

It must be emphasized that the review by the IPC was limited to personal health information collected, used and disclosed by the prescribed person pursuant to its function as a prescribed person under subsection 39(1)(c) of the *Act* and not with respect to any other role or responsibility that the prescribed person may have assumed under the *Act*.

Description of the INSCYTE Corporation

INSCYTE Corporation is a not-for-profit partnership of medical laboratories in the Province of Ontario and Cancer Care Ontario ("INSCYTE"). INSCYTE has developed and operates CytoBase, a computerized information system of cervical cytology and related test results in order to reduce the incidence and mortality from cervical cancer. INSCYTE in respect of CytoBase is a prescribed person within the meaning of subsection 39(1)(c) of the *Act*.

Three-Year Review of the INSCYTE Corporation

1. Privacy and Security Governance and Accountability Framework

The President of INSCYTE, who reports directly to the Board of Directors, is ultimately accountable for ensuring that INSCYTE complies with the *Act* and with the privacy and security policies, procedures and practices implemented. The President has designated an individual to act as the Privacy Officer in order to oversee the privacy and security program. The specific

responsibilities and accountabilities as between the President and the Privacy Officer of INSCYTE are set out in a privacy delegation chart that is reviewed on an annual basis.

The Privacy Officer is responsible for developing, implementing, reviewing and ensuring adherence to the privacy and security policies, procedures and practices implemented and for ensuring compliance with the *Act*. The Privacy Officer is also responsible for documenting, investigating and remediating privacy complaints and privacy breaches; for developing and delivering privacy and security training; and for ensuring the execution of confidentiality and data sharing agreements.

2. Overview of Privacy and Security Policies and Procedures

INSCYTE has developed a privacy policy in respect of CytoBase, the *Privacy Code Relating to the Collection, Protection, Use and Disclosure of Personal Health Information* ("the *Privacy Code*"). The *Privacy Code* describes the status of INSCYTE as a prescribed person within the meaning of subsection 39(1)(c) of the *Act* and the obligations that arise from this status and describes the purposes for which it collects, uses and discloses personal health information. The *Privacy Code* further sets out the accountability framework for ensuring compliance with the *Act* and for ensuring adherence to the privacy and security policies, procedures and protocols implemented. INSCYTE has also implemented numerous privacy and security policies, procedures and protocols that support the *Privacy Code*, including policies, procedures and protocols related to:

- Receiving, documenting, tracking, investigating and remediating privacy complaints;
- De-identification of personal health information;
- Linkage of personal health information;
- Retention and destruction of records of personal health information; and
- Reporting, managing, investigating and remediating privacy and security breaches.

Breach Protocol

INSCYTE has developed and implemented a *Breach Protocol* to address the identification, reporting, management, notification, investigation and remediation of breaches involving personal health information in CytoBase. The term "breach," however, is not defined in the *Breach Protocol*. It is recommended that the *Breach Protocol* be amended to provide a definition of "breach" and that the definition, at a minimum, include:

- The collection, use, disclosure, retention or disposal of personal health information in contravention of applicable laws, including but not limited to the *Act* and its regulation;
- A breach of any privacy and security policies, procedures and protocols implemented by INSCYTE from time to time; and/or

- A breach of the *Confidentiality and Non Disclosure Agreement* or the privacy terms and conditions in any other agreement between INSCYTE and its agents.

The *Breach Protocol* requires every person that discovers a breach, attempted breach or suspected breach to report the breach, attempted breach or suspected breach to the Privacy Officer and to the President of INSCYTE who will subsequently notify the Board of Directors. However, it is unclear what information with respect to the breach must be reported to the Privacy Officer and to the President and the format in which it must be reported. It is recommended that this be clarified.

The *Breach Protocol* also does not address containment of the breach. It is important that the process of containment be initiated immediately upon discovery of the breach, attempted breach or suspected breach in order to prevent further theft, loss or unauthorized access, use, disclosure, copying, modification or disposal of personal health information. It is recommended that the *Breach Protocol* be amended to address containment of the breach including who is responsible for containing the breach, the procedures to be followed in containing the breach, when containment must be commenced and the procedure for reviewing the containment measures implemented in order to determine if the breach has been effectively contained or whether further action is required.

The Board of Directors, or an appointee of the Board of Directors, is then responsible for investigating the breach, for determining the extent of the breach, for determining the actions that will be taken in response to a breach and for preparing an action plan. It is unclear what documentation will be maintained by INSCYTE with respect to the containment, investigation and remediation of breaches. Documentation of a breach is critically important for both managing breaches and for preventing similar breaches in future. It is therefore recommended that the *Breach Protocol* be amended to address the documentation of breaches.

The *Breach Protocol* states that where appropriate, the individuals to whom the personal health information relates will be advised of a breach. It is recommended that, as a secondary user of personal health information, INSCYTE notify the health information custodians that provided the personal health information in the event of a breach in order that the health information custodians may notify the individuals to whom the personal health information relates when required pursuant to subsection 12(2) of the *Act*, as opposed to INSCYTE notifying these individuals directly.

In addition, the *Breach Protocol* currently requires notification to be provided only in the event of a "significant" breach. It is recommended that the requirement for a breach to be "significant" prior to notification of the health information custodian be deleted due to the subjective nature of what constitutes a "significant breach" and due to the notification obligations imposed on INSCYTE pursuant to the *Data Sharing Agreements* with health information custodians from which it collects personal health information. Instead, INSCYTE should be required to notify the health information custodians who provided the personal health information whenever there is a breach, in order that the health information custodians may notify the individuals to whom the personal health information relates pursuant to subsection 12(2) of the *Act*.

In revising the *Breach Protocol*, INSCYTE may wish to have regard to the guidelines entitled *What to Do When Faced with a Privacy Breach: Guidelines for the Health Sector* produced by the IPC.

Security Breach Policy

INSCYTE has developed and implemented a policy governing security breaches involving personal health information in CytoBase, the *Reporting a Breach of Security Policy*, which requires all breaches or suspected breaches of security to be reported as soon as possible to the Privacy Officer.

However, once again, the term "security breach" is not defined. Further, the *Reporting a Breach of Security Policy* does not address the containment, notification, investigation and remediation of the security breach. Also, while the *Reporting a Breach of Security Policy* states that all security breaches or suspected security breaches must be reported to the Privacy Officer, it is unclear what information with respect to the security breach or suspected security breach must be reported and the format in which it must be reported.

It is recommended that the *Reporting a Breach of Security Policy* be amended to define what is meant by a "security breach," to indicate what information must be reported to the Privacy Officer in respect of a security breach or suspected security breach and to address containment, notification, investigation and remediation of the security breach.

Review of Privacy and Security Policies, Procedures and Protocols

The *Privacy Protocols and Procedures Governing the Collection, Use, Disclosure and Protection of Personal Health Information* ("the *Privacy Protocols and Procedures*") implemented by INSCYTE state that the *Privacy Code* and the *Privacy Protocols and Procedures* may be amended "at any time as appropriate" by the Privacy Officer, subject to the amendments being approved by the Board of Directors. However, the frequency for this review is not defined nor is the frequency of the review of the security policies, procedures and protocols implemented by INSCYTE. outlined

It is recommended that INSCYTE develop a policy and implement procedures for the annual review of its privacy and security policies, procedures and protocols. It is further recommended that this policy and these procedures set out the person(s) responsible for undertaking the review, the procedure to be followed in undertaking the review, the procedure to be followed in amending the policies, procedures and protocols and the time frame each year in which this review will be undertaken.

It is further recommended that the review of the privacy and security policies, procedures and protocols implemented have regard to technological advancements; to any orders, guidelines and best practices issued by the IPC; to any industry security and privacy best practices; and to any new or amendments to existing privacy legislation relevant to INSCYTE in respect of CytoBase, including amendments to the *Act* and its regulation. It is also recommended that in

undertaking this review, INSCYTE ensure that there are no inconsistencies between and among the various privacy and security policies, procedures and protocols implemented.

3. Information Available Related to Privacy and Security Policies and Procedures

INSCYTE makes information about its privacy and security policies, procedures and practices in respect of CytoBase readily available on its website, **www.inscyte.org**, including the *Privacy Code,* a brochure entitled *CytoBase and Your Right to Privacy*, Frequently Asked Questions and contact information for the individuals accountable for ensuring compliance with these policies, procedures and practices and to whom complaints or inquiries can be made. In addition, INSCYTE makes information available on its website related to the nature of the personal health information collected in CytoBase, the purposes for which it collects this personal health information and the persons and organizations from which it collects personal health information.

4. Collection, Use and Disclosure of Personal Health Information

Collection

INSCYTE in respect of CytoBase electronically collects personal health information from laboratories in the form of cervical cytology and related test results, such as colposcopy and biopsy results, at the same time that these test results are sent to the health care practitioners providing health care to the individuals. Prior to the collection of personal health information, INSCYTE requires that a *Data Sharing Agreement* be executed with the person or organization from which the personal health information will be collected.

The personal health information collected by INSCYTE for purposes of CytoBase includes the name, gender, date of birth, full contact information and health card number of the individual to whom the cervical cytology and related test results relate, the name and contact information of the health care practitioner that ordered the laboratory test, the name and contact information for the laboratory where the laboratory test was analyzed and information relating to the laboratory test, such as the type of test or analysis ordered, a description of the specimen collected and the results of the laboratory test.

Use

Personal health information collected for purposes of its function as a prescribed person under subsection 39(1)(c) of the *Act* is used for purposes of facilitating or improving the provision of health care. In particular, the personal health information is used for the purpose of ensuring abnormalities that can potentially develop into cervical cancer are detected and treated in a timely manner thereby reducing the incidence of cervical cancer.

The personal health information in CytoBase, namely the cervical cytology and related test results, is used by INSCYTE to produce monthly reminder letters to health care practitioners to ensure that their patients are being tested at appropriate intervals and to ensure that patients with abnormal results receive appropriate follow-up care and treatment in the prescribed time frame. The reminder letters are delivered to health care practitioners by the laboratory where the test was performed.

INSCYTE also uses the cervical cytology and related test results to produce aggregate statistics relating to cervical cancer screening in Ontario that are then used to plan and develop strategies for reducing the incidence of, and mortality from, cervical cancer in the Province of Ontario.

Currently, INSCYTE does not use personal health information for research purposes.

Disclosure

Personal health information contained within CytoBase is disclosed by INSCYTE for the purposes of facilitating or improving the provision of health care, including in the circumstances below.

INSCYTE discloses personal health information, namely historical cervical cytology and related test results of an identifiable individual, to a laboratory that is interpreting the current laboratory test of this same individual. This disclosure is made to facilitate and improve the provision of health care by enhancing the reliability and accuracy of test results. In particular, when analyzing a new specimen and determining the result of a current laboratory test, the laboratory retrieves the results of previous cervical cytology and related tests of this same individual from CytoBase, and analyzes and uses these previous tests results in order to interpret the cellular characteristics in the new specimen and to determine the result of the current laboratory test.

Prior to any such disclosure, the pathologist and other laboratory staff must complete, execute and submit an application form which contains standard terms and conditions governing the use of personal health information in CytoBase. Namely, the pathologist and laboratory staff must agree to only access the personal health information of individuals whose test results have been forwarded to them for review, to treat the personal health information in accordance with the *Act* and to notify INSCYTE of any breach or misuse of CytoBase.

INSCYTE also discloses personal health information in CytoBase, namely cervical cytology and related test results, to health care practitioners who subscribe to the "CytoBase for Clinicians Service" and who are providing health care to the individuals to whom these test results relate. This disclosure is made in order to facilitate the timely re-screening and follow-up of abnormalities. Prior to any such disclosure, the health care practitioner must complete, execute and submit an application form that contains standard terms and conditions governing the use of the personal health information. The health care practitioner must agree to only access the personal health information of individuals to whom he or she is providing health care and only with the consent of these individuals, to treat the personal health information in accordance with the *Act* and to notify INSCYTE of any breach or misuse of CytoBase.

In addition, INSCYTE discloses personal health information in CytoBase to Cancer Care Ontario, a prescribed entity within the meaning of section 45 of the *Act*, for purposes of analysis and compiling statistical information with respect to the management, evaluation, monitoring, allocation of resources or planning for the cervical cancer system. This disclosure is made pursuant to a *Data Sharing Agreement*.

INSCYTE also discloses aggregate information relating to cervical cancer screening in the Province of Ontario. Prior to the publication of aggregate information, the Privacy Officer is required, pursuant to the *Limiting Disclosure Protocol*, to review the aggregate information to assess the risk of inadvertent disclosure of personal health information.

Although the *Privacy Code* refers to the fact that the personal health information in CytoBase is made available for research purposes in accordance with the *Act* and its regulation, INSCYTE has indicated that it does not currently use or disclose personal health information for research purposes. It is recommended that in the event INSCYTE decides to use or disclose personal health information in CytoBase for research purposes, that INSCYTE develop policies, procedures and protocols with respect to the use and disclosure of personal health information for research purposes in accordance with the *Act* and its regulation prior to any such use or disclosure.

5. Retention and Destruction of Personal Health Information

INSCYTE retains records of personal health information in electronic format for as long as necessary to fulfill the stated purposes for which it was collected, namely to facilitate or improve the provision of health care pursuant to subsection 39(1)(c) of the *Act*. Records of personal health information in paper format are only retained for as long as necessary to transfer the personal health information into electronic format. INSCYTE has developed and implemented a *Destruction of Personal Health Information Protocol* that sets out the procedures to be followed in destroying records of personal health information in both paper and electronic format.

The *Destruction of Personal Health Information Protocol* requires that all records of personal health information in paper format be destroyed by shredding. However, it is unclear what type of shredding is employed. It is recommended that the *Destruction of Personal Health Information Protocol* be amended to set out the type of shredding that is employed and that the shredding employed be consistent with Order HO-001 and *Fact Sheet 10: Secure Destruction of Personal Information* issued by the IPC and with the definition of secure destruction in subsection 1(5.1) of Regulation 329/04 to the *Act*. The *Destruction of Personal Health Information Protocol* further requires that all records of personal health information in electronic format, such as CD, DVD, magnetic tape or floppy diskette, be physically destroyed thereby rendering the media unusable.

6. Administrative Safeguards Implemented

In addition to its privacy and security policies, procedures and protocols, INSCYTE has implemented the following administrative safeguards to protect personal health information against theft, loss and unauthorized use, disclosure, copying, modification or disposal.

Privacy and Security Training

INSCYTE has implemented an *Operational Security Protocol* that requires all agents of INSCYTE to undergo privacy and security awareness training provided by the Privacy Officer regardless of whether or not the agent will have access to personal health information. However, those agents who will have access to personal health information must undergo privacy and security training prior to being given access to personal health information.

This mandatory privacy and security awareness training is formalized in a PowerPoint presentation entitled *Privacy Policies, Procedures and Awareness*. This presentation discusses and explains the status of INSCYTE in respect of CytoBase as a prescribed person within the meaning of subsection 39(1)(c) of the *Act*, the *Privacy Code* implemented to protect the privacy of individuals whose personal health information is received and the requirements imposed on agents as a result of the *Privacy Code*.

The PowerPoint presentation also discusses the *Confidentiality and Non-Disclosure Agreement* that all agents of INSCYTE must execute, the *Breach Protocol* implemented by INSCYTE and the responsibility imposed on agents as a result of the *Confidentiality and Non-Disclosure Agreement* and the *Breach Protocol*. The privacy and security awareness training also discusses the roles and responsibilities of the Privacy Officer and the physical, administrative and technical safeguards implemented by INSCYTE and the responsibilities of agents in implementing these safeguards.

With respect to ongoing privacy and security training, the *Privacy Training Policy* states that the Privacy Officer is responsible for promoting privacy and security awareness and for promoting best practices with respect to safeguarding personal health information at every quarterly meeting.

It is unclear, however, how INSCYTE keeps track of attendance at both the initial and ongoing privacy and security awareness training, who is responsible for tracking attendance and the consequences for failing to attend. Further, it is unclear whether attendance at the ongoing privacy and security awareness training is mandatory and what the content is of this ongoing privacy and security awareness training, given that minutes are not taken at the quarterly meetings.

It is recommended that INSCYTE amend its *Operational Security Protocol* and *Privacy Training Policy* to explicitly stipulate that attendance at both the initial and ongoing privacy and security awareness training is mandatory and to implement procedures to track attendance, including who is responsible for tracking attendance and the consequences for failing to attend. It is further recommended that the ongoing privacy and security awareness training be formalized

and that it include role-based training in order to ensure that agents understand how to apply the privacy and security policies, procedures and practices implemented in their day-to-day work. It is also recommended that the ongoing privacy and security awareness training address any new privacy and security policies, procedures and practices implemented by INSCYTE and significant amendments to existing privacy and security policies, procedures and practices.

Confidentiality Agreements

The *Contractual Agreements Protocol* requires all agents of INSCYTE to sign a *Confidentiality and Non-Disclosure Agreement* upon the commencement of the relationship with INSCYTE and prior to being given access to personal health information, and thereafter on an annual basis. This includes the third party retained by INSCYTE to operate and maintain CytoBase.

However, it is unclear from a review of the documentation who is responsible for ensuring that the *Confidentiality and Non-Disclosure Agreement* has been executed, both initially and on an annual basis, how execution is tracked and the consequences for failing to execute the *Confidentiality and Non-Disclosure Agreement*. It is recommended that the *Contractual Agreements Protocol* be amended to formalize the practices and procedures related to the execution of the *Confidentiality and Non-Disclosure Agreement*.

By signing the *Confidentiality and Non-Disclosure Agreement*, agents acknowledge that as a result of their employment or contractual relationship with INSCYTE, that they may have access to personal health information. However, the *Confidentiality and Non-Disclosure Agreement* does not define personal health information nor does it address the uses and disclosures that may be made of the personal health information.

It is recommended that the *Confidentiality and Non-Disclosure Agreement* be amended to define personal health information in a manner consistent with the *Act* and to address the uses and disclosures that may be made of the personal health information. In particular, it is recommended that the agent acknowledge that personal health information will only be used when necessary for the purpose of carrying out the employment or contractual agreement and for no other purpose and will only be disclosed where permitted or required by law.

The *Confidentiality and Non-Disclosure Agreement* further requires agents to acknowledge that they have read, understood and agree to abide by the *Privacy Code* and the *Privacy Protocols and Procedures* and that a breach of the *Privacy Code* may result in disciplinary action, including termination of the employment or contractual relationship with INSCYTE. It is recommended that the *Confidentiality and Non-Disclosure Agreement* be amended to require an agent to acknowledge that a breach of not only the *Privacy Code*, but also the *Privacy Protocols and Procedures*, may result in disciplinary action. Further, it is recommended that the *Confidentiality and Non-Disclosure Agreement* be amended to require agents to notify the Privacy Officer for INSCYTE immediately, in writing, upon becoming aware of any breach of the *Confidentiality and Non-Disclosure Agreement*.

Data Sharing Agreements

The *Contractual Agreements Protocol* requires INSCYTE to enter into a *Data Sharing Agreement (CytoBase Site License)* prior to the collection of personal health information from health information custodians.

The *Data Sharing Agreement (CytoBase Site License)* sets out the purposes for which INSCYTE may use and disclose the personal health information collected and the administrative, technical and physical safeguards that will be implemented by INSCYTE to protect personal health information against theft, loss and unauthorized use, disclosure, copying, modification or disposal. It further requires INSCYTE to immediately notify the health information custodian, in writing, if personal health information is collected, used, disclosed, retained or disposed of in contravention of the *Act*, in contravention of the privacy and security policies, procedures and practices implemented or in contravention of the terms of the *Data Sharing Agreement (CytoBase Site License)*.

The *Contractual Agreements Protocol* also requires INSCYTE to enter into a *Data Sharing Agreement* prior to the disclosure of personal health information to any person or organization including health information custodians, agents of health information custodians and prescribed entities within the meaning of section 45 of the *Act*. In this regard, INSCYTE has developed a *Data Sharing Agreement (Data Recipient)* which must be executed prior to the disclosure of personal health information to health information custodians and their agents. The *Data Sharing Agreement (Data Recipient)* sets out the nature of the personal health information to be disclosed and the purpose for the disclosure of the personal health information.

It is recommended, however, that the *Data Sharing Agreement (Data Recipient)* be amended as set out in Appendix "C," to ensure uniformity in the terminology used, to limit the permitted uses and disclosures of personal health information by the Data Recipient, to ensure that the Data Recipient securely disposes of the personal health information and to clarify the obligation of the Data Recipient to notify INSCYTE in the event of a privacy breach.

Audit Program

INSCYTE conducts a number of reviews to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information including reviews of access rights to data holdings containing personal health information, reviews to ensure that personal health information is not being inappropriately stored on electronic media, reviews of audit logs and threat and risk assessments.

A record of agents having access to the personal health information in CytoBase is maintained, including the level of access, and is reviewed by the Privacy Officer on an annual basis to determine whether access is still required or whether it should be terminated, for example where the relationship between INSCYTE and the agent has ended. Further, one server, one computer, one workstation and one user account is randomly selected each month to ensure that personal

health information is not stored on unsecured servers, computers and workstations and to ensure that personal health information is not stored in emails or email attachments.

Further, all access to systems containing personal health information is recorded in a permanent audit log, as are all operations and actions that create, modify, delete or retrieve personal health information. Depending on the nature of the systems, the audit logs are reviewed on either a weekly or a daily basis. Any information in the audit logs that is indicative of a privacy breach, attempted privacy breach or suspected privacy breach must be immediately reported to the Privacy Officer.

These reviews, however, are not consolidated in one document. It is also unclear from a review of the documentation, with respect to each such review, what the mechanism and format is for reporting the findings of the review, to whom the findings of the review are reported and the procedure used in tracking the findings of the review and how the findings were addressed.

It is recommended that INSCYTE develop and implement a formal policy and associated procedures respecting the privacy and security audits conducted. It is further recommended that the policy or associated procedures set out the types of audits that will be conducted, the frequency of each audit, the procedure to be used in conducting each audit, the person responsible for conducting each audit, the mechanism and format for reporting the findings of each audit, to whom the findings of the audit will be reported and the procedure to track the findings of the audit and how each finding was addressed.

Policies Related to the Transmission of Personal Health Information

INSCYTE has implemented policies and procedures governing the transfer of personal health information that are documented in the *Privacy Policies and Procedures Regarding the Handling of Personal Health Information*. The *Privacy Policies and Procedures Regarding the Handling of Personal Health Information* require that every transfer of personal health information be recorded in a log which sets out the type of personal health information transferred, the date and time it was transferred, the intended recipient, the method of delivery, and if sent by courier or hand-delivered, the name of the person who retrieved the personal health information.

These policies and procedures also state that personal health information may not be transferred by facsimile transmission unless there is no other practical alternative, and only permit personal health information to be transferred by email transmission or secure file transfer if the personal health information is encrypted. However, these policies and procedures permit personal health information to be transferred in an unencrypted format if the personal health information is delivered by hand, by commercial bonded courier or by regular letter-mail in a sealed envelope.

It is recommended that INSCYTE amend its policies and procedures in order to ensure that personal health information is being transferred in a secure manner. In particular, it is recommended that the policies and procedures be amended to articulate the acceptable methods of transferring personal health information and to prohibit all other methods of transferring personal health

information, to set out the safeguards that must be employed in order to ensure that personal health information transferred through one of the acceptable methods is being transferred in a secure manner and to ensure that the acceptable methods of transferring personal health information and the safeguards employed are consistent with Order HO-004 and *Fact Sheet 12: Encrypting Personal Health Information on Mobile Devices* issued by the IPC.

7. Physical Safeguards Implemented

CytoBase is located in a locked facility with external video monitoring and tracked card access that divides the facility into varying levels of security with each successive level being more secure and restricted to fewer individuals. In order to access the server room, individuals must successfully pass through multiple levels of security. The facility is also equipped with an alarm system and security personnel outside regular business hours.

8. Technical Safeguards Implemented

In addition to the reviews conducted to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information, described earlier in this report under the heading "Administrative Safeguards Implemented," INSCYTE has implemented a number of technical safeguards to protect personal health information in its custody or control against theft, loss and unauthorized use, disclosure, copying, modification and disposal.

The technical safeguards implemented include the use of firewalls and network encryption and intrusion detection systems and the separation of the network over which personal health information is accessed from other networks. Personal health information is only transmitted through 128-bit asymmetric encryption that encrypts personal health information in transit and authenticates sending and receiving computer systems.

In addition, access to CytoBase is restricted by means of unique individual account names and passwords, account user registration, two level authentication and role-based restrictions.

All personal health information in paper format or on portable media is required to be stored in a secure location behind at least one security checkpoint. Further, upon the receipt of personal health information, the personal health information must be immediately transferred to the secure location and the receipt of the personal health information must be recorded in a log (including the date and time of receipt, the name of the sender, the name of the receiver and the nature of the personal health information).

Further, INSCYTE ensures that threat and risk assessments are conducted on its information technology infrastructure and related applications in order to identify real and potential threats, to assess vulnerabilities and to provide mitigation strategies. The most recent threat and risk assessment was conducted in June 2008.

Summary of Recommendations

It is recommended that INSCYTE in respect of CytoBase address the recommendations detailed in this report prior to the next review of its practices and procedures. In summary, it is recommended that INSCYTE:

1. In respect of its policies, procedures and practices relating to privacy and security breaches:

    (a) Amend the *Breach Protocol* to define the term "breach," to identify what information with respect to a breach must be reported to the Privacy Officer and the format for this report, to address containment of the breach, to outline the documentation that must be maintained with respect to the breach and to require the health information custodian who provided the personal health information to be notified of a breach; and

    (b) Amend the *Reporting a Breach of Security Policy* to define what is meant by a "security breach," to indicate what information must be reported to the Privacy Officer in respect of a security breach or suspected security breach and the format for this report and to address containment, notification, investigation and remediation of a security breach.

2. Develop and implement a written policy and associated procedures for the annual review of the privacy and security policies, procedures and protocols implemented by INSCYTE.

3. Develop written policies and procedures with respect to the use and disclosure of personal health information for research purposes in accordance with the *Act* and its regulation prior to any use or disclosure of personal health information for research purposes.

4. Amend the *Destruction of Personal Health Information Protocol* to set out the type of shredding that is employed for records of personal health information in paper format and ensure that the shredding employed is consistent with Order HO-001 and *Fact Sheet 10: Secure Destruction of Personal Information* issued by the IPC and with the definition of secure destruction in subsection 1(5.1) of Regulation 329/04 to the *Act*.

5. With respect to privacy and security awareness training:

    (a) Amend the *Operational Security Protocol* and *Privacy Training Policy* to explicitly stipulate that attendance at the initial and ongoing privacy and security awareness training is mandatory and to implement procedures to track attendance at the initial and ongoing privacy and security awareness training, including who is responsible for tracking attendance and the consequences for failing to attend; and

    (b) Formalize the ongoing privacy and security awareness training and ensure that the ongoing training includes role-based training and addresses new privacy and security policies, procedures and protocols implemented by INSCYTE and

significant amendments to existing privacy and security policies, procedures and protocols.

6. Amend the *Contractual Agreements Protocol* to formalize the practices and procedures related to the execution of the *Confidentiality and Non-Disclosure Agreement* and amend the *Confidentiality and Non-Disclosure Agreement* pursuant to the comments in this report.

7. Amend the *Data Sharing Agreement (Data Recipient)* in accordance with the comments set out on this report, including Appendix "C" to this report.

8. Develop and implement a written policy and associated procedures for the conducting of privacy and security audits.

9. Amend the *Privacy Policies and Procedures Regarding the Handling of Personal Health Information* to articulate the acceptable methods of transferring personal health information and to prohibit all other methods of transferring personal health information, to set out the safeguards that must be employed in order to ensure that personal health information transferred through one of the acceptable methods is being transferred in a secure manner and to ensure that the acceptable methods of transferring personal health information and the safeguards employed are consistent with Order HO-004 and *Fact Sheet 12: Encrypting Personal Health Information on Mobile Devices* issued by the IPC.

Statement of Continued Approval of Practices and Procedures

The IPC is satisfied that INSCYTE in respect of CytoBase continues to have in place practices and procedures that sufficiently protect the privacy of individuals whose personal health information it receives and that sufficiently maintain the confidentiality of that information. Accordingly, effective October 31, 2008, the IPC is satisfied that INSCYTE continues to meet the requirements of the *Act*.

APPENDIX "A"

RECOMMENDATIONS FROM THE INITIAL REVIEW

The IPC made the following recommendations during the initial review of the practices and procedures implemented by INSCYE in respect of CytoBase that were approved by the IPC effective October 31, 2005:

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

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 the *Act* 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.

APPENDIX "B"

DOCUMENTATION REQUESTED

Privacy

- Privacy policies and procedures and the mechanism for reviewing and updating these policies and procedures
- Overview of privacy program and privacy audit program
- Reports on internal or external privacy audits conducted or completed
- Policies, procedures and protocols for privacy breaches and complaints
- Policies, procedures and protocols for data de-identification and data linkage including when, how, the purposes for which and by whom it will be de-identified or linked
- Information about the privacy training program for new and current employees, affiliates and volunteers including when it is provided, its content (copies of training material) and the mechanism to ensure that employees, affiliates and volunteers have been trained
- Information available to the public relating to privacy (i.e. brochures, frequently asked questions) and where it is made available
- Policies, procedures, protocols and agreements relating to research
- Privacy impact assessments for data holdings or programs including information relating to whether privacy impact assessments have been completed for all data holdings or programs, and if not, which have been completed and which remain outstanding

Security

- Security policies and procedures setting out the administrative, technical and physical safeguards and the mechanism for reviewing and updating these policies and procedures
- Policies, procedures and protocols for ensuring that personal health information is protected against theft, loss and unauthorized use or disclosure, including:
    - access control (authentication/authorization)
    - perimeter control, electronic control
    - encryption, firewalls and virus scanners

- secure transfer procedures
- password policies
- audit trails

- Information about the nature, scope and frequency of audits of access to data holdings
- Policies, procedures, protocols and agreements related to the secure retention, disposal and destruction of personal health information including retention schedules
- Policies, procedures and protocols related to sending and receiving personal health information including by facsimile, email transmission and other methods
- Policies, procedures and protocols for personal health information on portable or mobile devices such as laptop computers, personal digital assistants and flash drives
- Reports on internal or external threat and risk assessments
- Business continuity and disaster recovery plans
- Information about the security training program for new and current employees, affiliates and volunteers including when it is provided, its content (copies of training material) and the mechanism to ensure employees, affiliates and volunteers have been trained
- Reports on internal or external security audits conducted or completed

Organizational and Other Documentation

- Inventory of data holdings of personal health information
- Respective roles and responsibilities for privacy and security including information about the appointed contact persons for privacy and security and to whom they report and information about the terms of reference for privacy and security committees
- Confidentiality, non-disclosure, data sharing, research and third party agreements
- Policies, procedures and protocols relating to the execution of these agreements, including procedures to track and monitor their execution
- Disciplinary policies/procedures for violations
- Detailed documentation evidencing the completion of each recommendation set out in the report of the Information and Privacy Commissioner of Ontario dated October 2005

APPENDIX "C"

RECOMMENDED AMENDMENTS TO THE *DATA SHARING AGREEMENT (DATA RECIPIENT)*

Inconsistent Use of Terminology to Describe the "Data"

The *Data Sharing Agreement (Data Recipient)* uses the terms "data," "personally identified data," "information" and "cervical cytology results" interchangeably and it is not clear whether there is a distinction between these terms and, if so, the basis for this distinction. It is recommended that if there is a distinction between these terms, that each term be appropriately defined, and that if there is no such distinction, that one term be used consistently and that the term be appropriately defined.

Section 1.3 – Intended Use of the Information

Section 1.3 identifies the intended uses of the "data" or "information" but it is unclear by whom these intended uses are to be made. It is recommended that this section be amended to make clear that these intended uses will be made by INSCYTE. The permitted uses by the Data Recipient should instead be addressed in section 2.4. It is also recommended that it be made explicit that the "data" or "information" will only be used in accordance with the *Act* and its regulation.

Section 1.5 – Release of Data

Section 1.5 states that "data" may be released to entities approved by INSCYTE, subject to a *Data Sharing Agreement*, for the purpose of enhancing the reliability and accuracy of future test results, of monitoring the efficacy of health care services performed and of providing information relevant to screening programs and epidemiological studies. It is unclear by whom this release of data may be made. It is recommended that this section be amended to make clear that this release of data will be made by INSCYTE and that the permitted disclosures by the Data Recipient be addressed in section 2. It is also recommended that it be made explicit that this release of data will only be made in accordance with the *Act* and its regulation.

Section 2.1 – Engaged in Preventative Activities

Section 2.1 states that if the Data Recipient ceases to be actively engaged in activities directed at the prevention of cervical cancer it is required to inform INSCYTE within thirty days. It is not clear however, what the consequence would be if the Data Recipient ceased to be actively

engaged in such activities. This should be made explicit in the *Data Sharing Agreement (Data Recipient)*.

Section 2.2 – Authorization Required

Section 2.2 states that the Data Recipient warrants that it has the authority to receive the "data." It is recommended that this statement be amended to require the Data Recipient to not only warrant that it has the authority to receive the "data" but that its receipt of the "data" is in compliance with the *Act* and its regulation given that, as a prescribed person for purposes of subsection 39(1)(c) of the *Act*, INSCYTE may only disclose personal health information in accordance with the *Act*.

Section 2.5 – Records

While the *Data Sharing Agreement (Data Recipient)* contains limitations on the collection and use of the "data" or "information" by the Data Recipient, it does not contain limitations on the disclosure of the "data" or "information." Section 2.5 simply requires the Data Recipient to maintain records of the persons to whom the "data" or "information" was disclosed and the date of the disclosure. It is recommended that this section be amended to explicitly state that any disclosure of the "data" or "information" must comply with the *Act* and its regulation.

Section 2.6 – Destruction of Data

Section 2.6 requires the Data Recipient to destroy the "data" within thirty days of the time it is no longer required and within thirty days of the time it ceases to be actively engaged in activities directed at the prevention of cervical cancer. It is recommended that this section be amended to make explicit that the data must be destroyed in a secure manner and to provide a definition of secure destruction consistent with subsection 1(5.1) of Regulation 329/04 to the *Act*.

Further, in circumstances where the destruction results from the Data Recipient ceasing to be actively engaged in activities directed at the prevention of cervical cancer, the requirement for notification that the "data" has been destroyed should be amended to require the notification of destruction to set out the date, time and method of secure destruction employed and to require the notification to bear the signature of the person who performed the secure destruction.

Section 2.7 – Breach of Privacy

Section 2.7 requires the Data Recipient to immediately notify INSCYTE, in writing, in the event of a "breach of privacy." The term "breach of privacy" however, is not defined. It is recommended that the term "breach of privacy" be defined and that it be defined in a manner consistent with the *Data Sharing Agreement (CytoBase Site License)*.

Section 3.3 – Security Administration

Section 3.3 states that in the event of a breach or attempted breach, INSCYTE reserves the right to suspend or terminate the *Data Sharing Agreement (Data Recipient)*. It is recommended that this statement be amended to ensure consistency with section 2.7. In particular, it is recommended that section 3.3 be amended to state that in the event of a breach of privacy or suspected breach of privacy by the Data Recipient, as defined in section 2.7, INSCYTE reserves the right to suspend or terminate the *Data Sharing Agreement (Data Recipient)*.

It is further recommended that section 3.3 be amended to state that in the event of a suspension or termination of the *Data Sharing Agreement (Data Recipient)* as a result of a breach or suspected breach of privacy by the Data Recipient, the Data Recipient shall, within ten days of the suspension or termination, destroy the "data" in a secure manner and provide INSCYTE with a notification of destruction setting out the date, time and method of secure destruction employed and bearing the signature of the person who performed the secure destruction. Section 3.3 should also be amended to define secure destruction and the definition adopted should be consistent with subsection 1(5.1) of Regulation 329/04 to the *Act*.

Section 4.0 – Expiry and Other Termination

Sections 4.1 and 4.2 govern the termination of the *Data Sharing Agreement (Data Recipient)* both in the event of a breach and where there has been no breach. However, none of these sections address how the termination of the *Data Sharing Agreement (Data Recipient)* affects the "data" or "information" in the possession of the Data Recipient. It is recommended that this be addressed in the *Data Sharing Agreement (Data Recipient)* and that the treatment of "data" or "information" be consistent with section 3.3 of the *Data Sharing Agreement (Data Recipient)*.