Inscyte Corporation

In Respect of CytoBase

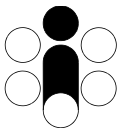
Report to the Information and Privacy Commissioner of Ontario
Three-Year Review as a Prescribed Person under *PHIPA*
Year of Submission (2020)

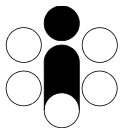
October 2020

Inscyte Corporation

Dr. Allan Seidenfeld – President and CEO
Jack Golabek – Privacy Officer

Table of Contents





Background Information

About Inscyte Corporation

Inscyte Corporation is a not-for-profit partnership of Ontario medical laboratories. In 1996, Inscyte Corporation began operating "**CytoBase**", a centralized database of patient identified cervical cancer screening test results gathered from member laboratories. The personal health information that Inscyte Corporation collects is used for improving patient care and serves four purposes:

1. **CytoBase** provides patient-related historical test results to laboratory personnel that are reading new Pap tests, regardless of where in Ontario the previous tests were performed. Since cervical cancer is a slowly progressing disease, the availability of historical results on individual women is important in the interpretation of new smears. Also, historical results are essential for laboratory quality assurance and for planning patient follow-up.

2. **CytoBase** supports the work of the Ontario Cervical Cancer Screening Program, which is administered by Ontario Health. Screening test results received from participating laboratories are forwarded to Ontario Health daily for incorporation into Ontario Health's Integrated Cancer Screening system (ICS).

3. **CytoBase** produces monthly physician reminder letters to ensure that women are tested at appropriate intervals and that women with abnormal results receive follow-up in the appropriate time frame. Written reminder letters are delivered to physician offices by member laboratories courier networks.

4. Personal health information in **CytoBase** is periodically aggregated to produce statistics describing the utilization and trends of cervical cancer screening in Ontario.

Inscyte Corporation also provides a secure online service for primary care providers. This service is called "CytoBase for Clinicians" and permits authorized physicians, nurse practitioners and midwives to access screening histories and follow-up status on individual patients within their care.

Ontario Regulation 329/04 made under the *Personal Health Information Protection Act, 2004* (the Act) designates Inscyte Corporation in respect of CytoBase as a Prescribed Person under section 39(1)(c) of the Act.

About Artificial Intelligence in Medicine Inc. (now Inspirata Canada Inc.)

Artificial Intelligence in Medicine Inc. was acquired by Inspirata Inc. in January 2018. Inspirata Inc. is a global cancer informatics company headquartered in Tampa, Florida. In July 2019, Artificial Intelligence in Medicine Inc. changed its corporate name to Inspirata Canada Inc., hereinafter referred to as "Inspirata". This acquisition did not result in any material changes to staff or operations. Inspirata continues to implement the policies and procedures of Inscyte Corporation in respect of CytoBase with the same accountabilities and staff responsibilities.

Inspirata is a privately held software engineering firm located in Toronto, Ontario. Inspirata develops information technology solutions for healthcare industry with a special focus on cancer research and prevention. Inspirata has clients throughout Canada, the U.S., and Australia.

Inscyte Corporation has contracted Inspirata for the maintenance, upgrades, quality assurance, and administrative work required in the day-to-day operations of the CytoBase system since its inception in 1996. The CytoBase database is physically located at Inspirata's secure datacenter. Inspirata is also responsible for maintaining the network reporting infrastructure (i.e. laboratory connections) for CytoBase and hosting the Inscyte website and the "CytoBase for Clinicians" online application.

Since Inspirata works in the healthcare domain its staff routinely handles personal health information, not only that of Inscyte Corporation, but from many other clients as well. As such, Inspirata itself has a comprehensive privacy and security program in place. This program implements Inscyte Corporation's Privacy & Security Policies and Procedures.

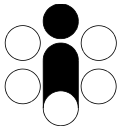
Contact Information

Please direct all inquiries to:

Jack Golabek, P.Eng
Privacy Officer – Inscyte Corporation

c/o
Inspirata Canada Inc. (formerly Artificial Intelligence in Medicine Inc.)
2 Berkeley Street, Suite 403
Toronto, Ontario
M5A 2W3

Tel: 416-594-9393
Email: inscyte@inspirata.com



Part 1 – Privacy Documentation

1. Privacy Policy in Respect of Inscyte Corporation's Status as a Prescribed Person

Inscyte Corporation has a comprehensive Privacy Policy in effect in relation to personal health information it receives and uses with respect to its status as a prescribed person under Ontario's Personal Health Information Protection Act, 2004 ("the Act"). The Privacy Policy is articulated in two overarching documents: Inscyte's *Privacy Code* and its *Privacy & Security Policies and Procedures Manual.*

Status under the Act

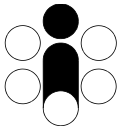
The Privacy Policy describes Inscyte Corporation a prescribed person under the Act and the duties and responsibilities that arise as a result of this designation. The Privacy Policy indicates that Inscyte Corporation has implemented policies, procedures and practices to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information and that these policies, procedures and practices are subject to review by the Information and Privacy Commissioner of Ontario every three years.

The Privacy Policy describes Inscyte's commitment to comply with the provisions of the Act and its regulation and describes Inscyte's accountability framework for ensuring compliance with the Act and its regulation, and for ensuring compliance with its privacy & security policies and procedures.

Privacy and Security Accountability Framework

The President of Inscyte Corporation is ultimately accountable for ensuring compliance with the Act and its regulation, and for ensuring compliance with Inscyte's Privacy & Security Policies and Procedures. The President reports to the Board of Directors of Inscyte Corporation, which is comprised of representatives of the medical laboratories (health information custodians) that provide personal health information to Inscyte Corporation.

The Privacy Policy identifies the position of Privacy Officer as having day-to-day authority to manage the privacy program and Inspirata's Security Officer as having day-to-day authority to manage the security program. The Privacy Policy also defines the responsibilities of these positions. Inscyte's Privacy Officer reports to the President of Inscyte. Inspirata's Security Officer reports to the Chief Executive Officer of Inspirata. Inspirata, as agent of Inscyte, is responsible for implementing Inscyte's Privacy Policy. Inspirata's Chief Executive Officer is accountable to the President of Inscyte for ensuring Inspirata's compliance with Inscyte's privacy & security policies and procedures.



Collection of Personal Health Information

The Privacy Policy describes the purpose for which Inscyte collects personal health information, the type of personal health information it collects, and the organizations from which it collects the information. The Privacy Policy further specifies that the collection of personal health information must be consistent with the collection of personal health information permitted by the Act and its regulation.

The Privacy Policy states that Inscyte will not collect personal health information if other information will serve the purpose. The Privacy Policy also states that Inscyte only collects personal health information for its stated purpose and that it collects the minimum amount of personal health information required to fulfill its stated purpose. Inscyte's privacy & security policies and procedures ensure that both the amount and the type of personal health information collected is limited to that which is reasonably necessary for its stated purpose.

Inscyte's Privacy Policy includes the requirement to maintain a list of its data holdings of personal health information and identifies the Privacy Officer as the contact for obtaining further information in relation to the purposes, data elements, and data sources of each data holding.

Use of Personal Health Information

The Privacy Policy also describes the purpose for which Inscyte uses personal health information and includes policies and procedures that distinguish between the use of personal health information under section 39(1)(c) of the Act and the use of de-identified and/or aggregate information. The Privacy Policy also states that Inscyte Corporation does not use personal health information for research purposes. As such, Inscyte does not disclose personal health information to researchers or agents. The Privacy Policy further specifies that the use of personal health information must be consistent with the uses of personal health information permitted by the Act and its regulation.

The Privacy Policy states that Inscyte will not use personal health information if other information will serve the purpose and will not to use more personal health information than is reasonably necessary to meet the purpose. Policies and procedures have been implemented in this regard to establish limits on the use of personal health information from CytoBase by participating laboratories and other organizations.

Disclosure of Personal Health Information

The Privacy Policy identifies the purposes for which personal health information is disclosed, the organizations to whom information is disclosed and the requirements that must be satisfied prior to such disclosures. Inscyte ensures that each disclosure is consistent with the disclosures of personal health information permitted by the Act and its regulation.

The Privacy Policy distinguishes between the purpose for which and the circumstances in which personal health information is disclosed and the purposes for which and the circumstances in which de-identified and/or aggregate information is disclosed. The privacy policies and procedures address methods of de-identification and aggregation to ensure that the information could not be utilized, either alone or with other information, to identify an individual. Inscyte's policy is to review all de-identified and/or aggregate information prior to disclosure to ensure that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. Furthermore, Inscyte's policy states that it will not disclose personal health information if other information will serve the purpose and that it will not disclose more personal health information than is necessary to meet the purpose of the disclosure.

Secure Retention, Transfer and Disposal of Records of Personal Health Information

The Privacy Policy addresses the secure retention of records of personal health information in paper and electronic format, including the acceptable use of portable media and mobile devices for the collection, transfer, and storage of personal health information. The Privacy Policy addresses the permitted retention periods and specifies methods for the secure transfer and destruction of personal health information depending on the media on which it is stored.

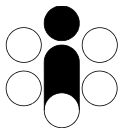
Implementation of Administrative, Technical and Physical Safeguards

The Privacy Policy also specifies Inscyte's security measures to safeguard personal health information and protect the privacy of individuals to whom the information pertains. The policies and procedures cover administrative, physical, and technical security controls implemented to protect personal health from unauthorized access, copying, modification, use, disclosure, theft, loss and improper disposal.

Inquiries, Concerns or Complaints Related to Information Practices

The Privacy Policy identifies the Privacy Officer of Inscyte as the contact to whom individuals may direct inquiries, concerns or complaints related to the privacy policies, procedures and practices of Inscyte and questions related to Inscyte's compliance with the Act and its regulation. The Privacy Policy specifies that the contact information will be provided on Inscyte's website and that a standard Inquiry or Compliance Challenge form will be made available to the public for lodging inquiries or complaints. This information has been available on Inscyte's website since 2011 and is currently available.

The Privacy Policy also states that individuals may direct complaints regarding Inscyte's compliance with the Act and its regulation to the Information and Privacy Commissioner of Ontario and that Inscyte will provide the mailing address and contact information for the Information and Privacy Commissioner of Ontario.



Transparency of Practices in Respect of Personal Health Information

The Privacy Policy commits Inscyte to be transparent about its practices in respect of handling personal health information and states that Inscyte shall make its Privacy Policy (Privacy Code and Privacy & Security Policies and Procedures Manual), together with FAQs and other relevant documents, freely available to the public from its website.

2. Policy and Procedures for Ongoing Review of Privacy Policies, Procedures and Practices

Inscyte's Privacy & Security Policies and Procedures Manual includes policies and procedures governing the regular review of its privacy policies, procedures, and practices. The policies state that Inscyte shall review its privacy program at minimum on an annual basis, or more frequently should there be changes in technology, best practices, the Act, and its regulation. The policies further state that a review of relevant policies and procedures shall be taken following a breach of privacy or security to determine if modifications to the policies and procedures are necessary to avert a similar breach in the future.

The policies state that it is the responsibility of the Privacy Officer to initiate a review process, that a committee shall be organized to carry out the review, and that in the event that proposed changes represent a material change to daily operations, the results and recommendations of the review will be reported to the President of Inscyte and CEO of Inspirata. for review and approval before the changes are implemented.

The policies state that the review process shall take into account any orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation; evolving industry privacy standards and best practices; amendments to the Act and its regulation relevant to the prescribed person or prescribed entity; and recommendations arising from privacy and security audits, privacy impact assessments and investigations into privacy complaints, privacy breaches and information security breaches. The review process also addresses whether the existing privacy policies and procedures continue to be consistent with actual practices and whether there is consistency between and among the privacy and security policies, procedures and practices implemented.

The policies describe the procedure for amending and documenting policies and procedures and for communicating the amendments to agents and the public. Amended policies and procedures result in a revision of Inscyte's Privacy & Security Policies and Procedures Manual, which is made available through Inspirata's internal business network and to the public on Inscyte's website. Inscyte's agent, Inspirata, is responsible for communicating amended policies and procedures and reviewing communication materials.

Compliance with the Privacy & Security Policies and Procedures is mandatory for all agents of Inscyte. Compliance is monitored by Inscyte's Privacy Officer and Security Officer. The Privacy Policy specifies that a contravention of the policies and procedures constitutes a breach and includes policies and procedures for corrective actions to be taken in the event of non-compliance.

The Privacy Policy includes policies and procedures governing Inscyte's privacy audit program. The policies state that Inscyte shall conduct an annual privacy audit that involves reviewing its inventory of personal health information holdings; reviewing access rights and uses of the personal health information; reviewing privacy logs for completeness and accuracy, including the Log of Privacy Training Sessions and Attendance, Log of Privacy Breaches, Log of Privacy Complaints, Log of Security Breaches, Log of Transfers of personal health information, Log of Data Holdings and Log of Individual's Access to personal health information.

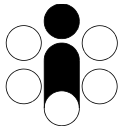
In addition, Inscyte's policy is to conduct a monthly random audit of computers, servers, and agent workspaces to detect potential breaches and non-compliance with its policies and procedures.

3. Policy on the Transparency of Privacy Policies, Procedures and Practices

Inscyte's Privacy Policy states that Inscyte is committed to maintaining the transparency of its privacy and security practices by making the following information available freely and openly to the public on its website:

1. Privacy Code
2. Privacy & Security Policies and Procedures
3. Privacy Brochure
4. Answers to Frequently Asked Questions (FAQ)
5. Documentation related to the review of Inscyte Corporation by the Information and Privacy Commissioner of Ontario in respect of Inscyte's policies, procedures and practices implemented to protect the privacy of individuals whose personal health information it holds and to maintain the confidentiality of that information
6. A list of the data holdings of personal health information maintained by Inscyte
7. A summary of privacy impact assessments
8. The name, title, mailing address and contact information of the persons(s) to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with the Act and its regulation may be directed

This information has been available on Inscyte's website since 2011 and is currently available. In addition, the policy specifies the minimum content of Inscyte Corporation's Privacy Brochure as follows:



1. The status of Inscyte Corporation under the Act
2. Inscyte's obligations under the Act
3. The type of personal health information collected
4. The organizations from which personal health information is collected
5. The purpose for which personal health information is collected
6. The purpose for which personal health information is used
7. The circumstances under which personal health information is disclosed
8. The entities to whom personal information is disclosed
9. Summary of administrative, physical and technical security controls including the steps taken to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal
10. The name and/or title, mailing address and contact information of the person(s) to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with the Act and its regulation may be directed

The policy in respect to the transparency of policies and procedures states that the President of Inscyte is responsible for ensuring that the above information is published on Inscyte's website.

4. Policy and Procedures for the Collection of Personal Health Information

Inscyte has policies and procedures that identify the purposes for which personal health information is collected, the nature of the personal health information that is collected, the health information custodians from whom the personal health information is collected and the secure manner in which personal health information is collected. Since CytoBase is an electronic medical record of cervical cancer screening tests/results the nature of the personal health information collected and the purpose for which it is collected does not change over time.

The Privacy Policy states that Inscyte Corporation collects patient identified laboratory test results pertaining to the screening and follow-up of cervical cancer for the purpose of improving patient care in Ontario by:

1. Compiling longitudinal patient screening histories and providing these to participating laboratories for quality improvement purposes when performing new tests.
2. Notifying primary care providers about overdue patient follow-up activities.
3. Supporting the Ontario Cervical Cancer Screening Program (operated by Ontario Health).
4. Producing aggregate statistics describing cervical cancer screening patterns and trends in Ontario.

Inscyte's policies articulate a commitment not to collect personal health information unless the collection is permitted by the Act and its regulation, not to collect personal health information if other information will serve the purpose and not to collect more personal health information than is reasonably necessary to meet the purpose. Inscyte only collects personal health information that is required for its stated purposes and does not collect more personal health information than is necessary to meet the stated purposes.

Personal health information is collected on an on-going daily basis from participating laboratories that perform the screening and follow-up tests. Inscyte requires participating laboratories to comply with its policies and procedures by executing a legally binding Data Sharing Agreement with each participating laboratory. Compliance with these agreements is enforced by the Inscyte Board of Directors, which is comprised of representatives from each of the participating laboratories. Inscyte also has a legally binding agreement with Inspirata. for the on-going operations and support of the CytoBase system that requires Inspirata, as its Agent, to implement and comply with Inscyte's privacy & security policies and procedures. Compliance with this agreement is also enforced by the Board of Directors of Inscyte which includes a representative from Inspirata.

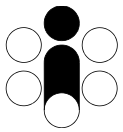
Compliance with the policies and procedures for the collection of personal health information are audited in accordance with Inscyte's policies and procedures in respect of privacy audits, which state that privacy audits are carried out at minimum on an annual basis and identifies the Privacy Officer of Inscyte and Inspirata's Security Officer as being responsible for conducting the audits and for ensuring day-to-day compliance with the privacy & security policies and procedures.

Inscyte's policies and procedures for managing privacy breaches require that agents of Inscyte and participating laboratories notify the Privacy Officer of Inscyte at the first reasonable opportunity if a breach, or suspected breach, of privacy has occurred. The definition of a breach of privacy includes the failure to comply with Inscyte's privacy & security policies and procedures.

Review and Approval Process

The policy and procedures state that the President of Inscyte is responsible for reviewing and determining whether to approve the collection of personal health information and to execute a Data Sharing Agreement with the provider of the information prior to the collection of personal health information. Executing a Data Sharing Agreement requires the approval of the Board of Directors of Inscyte.

The policy and procedures set out the criteria that must be considered for determining whether to approve the collection of personal health information. The criteria require that the collection be permitted under the Act and its regulation and that any and all conditions or restrictions set out in the Act and its regulation have been satisfied. The criteria also require determining



whether other information, such as de-identified and/or aggregate information, will serve the identified purpose such that no more personal health information is being requested than is reasonably necessary to meet the identified purpose.

The Privacy Policy states that collection of personal health information requires executing a Data Sharing Agreement between Inscyte and the provider(s) of the information. As such, the ultimate decision of whether or not to approve the collection of personal health information rests with the Board of Inscyte and the provider of the information, taking into account the criteria that must be considered in the review and approval process. The decision to approve or deny a request for the collection of personal information is communicated and documented by the parties during the process of establishing a Data Sharing Agreement.

Conditions or Restrictions on the Approval

The policy and procedures state that no personal health information shall be collected in the absence of a legally binding Data Sharing Agreement between Inscyte Corporation and the provider of the information and that all Data Sharing Agreements shall have regard to the requirements of the Act and its regulation. Furthermore, the policies require that each data holding be documented with a Statement of Purpose, a Statement of Permitted Use, and a Statement of Retention. It is the responsibility of the President of Inscyte to ensure that these conditions have been met prior to the collection of personal health information.

Secure Retention

Inscyte's Privacy Policy requires that records of personal health information are retained in a secure manner and includes policies and procedures addressing and restricting the secure storage of personal health information on paper records, portable media, mobile devices, email, and computer file/database systems. The personal health information collected by Inscyte is stored in the CytoBase database system housed within a secured datacenter with restricted access in accordance with the policies and procedures for the secure retention of personal health information.

Secure Transfer

Inscyte's Privacy Policy requires that records of personal health information are transferred in a secure manner and includes policies and procedures addressing and restricting the secure transfer of personal health information using paper records, portable media, mobile devices, email, and computer file/database systems. The day-to-day collection of personal health information from participating laboratories is accomplished by secure encrypted electronic transfer which does not involve human intervention and is in accordance with the policies and procedures for the secure transfer of personal health information.

Secure Return or Disposal

The policy and procedures identify the Privacy Officer of Inscyte as being responsible for ensuring that records of personal health information that have been collected are either securely returned or securely destroyed upon expiry of the retention period as documented in the Statement of Retention for the data holding of the personal health information in question. In general, the personal health information in CytoBase is retained in perpetuity.

Under the provisions of section 39(1)(c) of the Act and its regulations, Inscyte Corporation is a prescribed person who compiles and maintains a registry of personal health information (CytoBase) for purposes of facilitating and improving the provision of health care, specifically with respect to the screening and prevention of cervical cancer. Since cervical cancer is a slowly progressing disease, conditions that may lead to cancer must be monitored in individuals over their lifetime and be made available to pathologists and clinicians as needed to inform and improve patient care. A population-based historical record is also needed to understand patterns in disease progression and the efficacy of interventions and their outcomes. It is for this reason that Inscyte's policy is to retain the information in perpetuity.

The Privacy Policy states that records of personal health information that are to be returned to the organization from which they were collected must be returned in accordance with the policies and procedures for the secure transfer of personal health information.

The Privacy Policy states that records of personal health information that are to be destroyed at the expiry of the retention period must be destroyed in accordance with the policies and procedures for the secure disposal of personal health information.

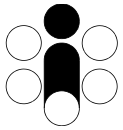
5. List of Data Holdings Containing Personal Health Information

Inscyte Corporation retains an up-to-date list and summary description of the data holdings of personal health information maintained by Inscyte.

6. Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information

Inscyte Corporation has policies and procedures governing the creation, review, amendment and approval of statements of purpose for data holdings containing personal health information. The policy and procedures require the statements of purpose to describe the purpose of the data holding, the personal health information contained in the data holding, the source(s) of the personal health information and the need for the personal health information in relation to the identified purpose.

The policy and procedures specify that the Privacy Officer is responsible for maintaining up-to-date statements of purpose and describe the process to be followed in completing the



statements of purpose for the data holdings containing personal health information. The policy and procedures require that the source(s) of the data holdings be consulted in completing the statements of purpose and specify that the President of Inscyte is responsible for approving the statements of purpose. The day-to-day authority to manage the privacy program in respect of the statements of purpose has been delegated to the Privacy Officer.

The policy and procedures state that statements of purpose are made available to the health information custodians from whom personal health information is collected—in particular, the medical laboratories that provide test results to CytoBase.

The policy and procedures require that the statements of purpose be reviewed in conjunction with regular annual reviews of the privacy program to ensure their continued accuracy and in order to ensure that the personal health information collected for purposes of the data holding is still necessary for the identified purposes.

The policies and procedures specify that the Privacy Officer is responsible for the annual review of statement of purpose and the process to be followed in reviewing the statements of purpose and in amending the statements of purpose. The policy and procedures require that the source(s) of the data holdings be consulted when amending the statements of purpose and specify that the President of Inscyte is responsible for approving amended statements of purpose. The policy and procedures state that amended statements of purpose are to be made available to the health information custodians from whom personal health information is collected—in particular, the medical laboratories that provide test results to CytoBase.

Inscyte requires is agents to comply with the policy and procedures. Compliance is monitored by the Privacy Officer in accordance with Inscyte's policies and procedures in respect of on-going privacy/security audits, which addresses the consequences of breach. The policy and procedures stipulate that audits are performed on a monthly basis. The Security Officer is responsible for conducting the audits and the Privacy Officer is responsible for ensuring compliance with the policy and its procedures.

The policy and procedures require agents to notify the Privacy Officer of Inscyte at the first reasonable opportunity of a breach or potential breach of privacy, in accordance with Inscyte's policies and procedures for identifying a breach of privacy, reporting a breach of privacy and actions to be taken following a breach of privacy.

7. Statements of Purpose for Data Holdings Containing Personal Health Information

Inscyte's policies and procedures require that a statement of purpose be documented and retained in the privacy document archives for each data holding containing personal health

information, identifying the purpose of the data holding, the personal health information contained in the data holding, the source(s) of the personal health information and the need for the personal health information in relation to the identified purpose.

8. Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information

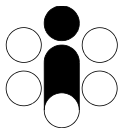
Inscyte Corporation has policies and procedures in place to limit access to and use of personal health information by its agents. The Privacy Officer is responsible for receiving, assessing, and approving or denying requests for access to, or use of, personal health information. The policies and procedures prescribe that access and use of personal health information shall be limited to select individuals on the basis of the "need to know" principal. The policies and procedures further stipulate that the scope of personal health information used in day-to-day work shall be limited to the least identifiable information and minimum amount of information required to complete the work.

Inscyte's policy and procedures limit the scope of work requiring access to personal health information to a narrow set of specific tasks having to do with the manual correction of lab reports, producing monthly follow-up notification letters for Ontario healthcare practitioners, and performing authorized data linkages with health information custodians or other prescribed persons or entities.

CytoBase is a centralized electronic medical record and owing to the highly limited scope of work that requires access to personal health information, only a few individuals are granted access to CytoBase. Furthermore, these individuals are granted different functional privileges to prevent a single individual from compromising personal health information.

For all other purposes and in all other circumstances, the policy and procedures require agents to access and use de-identified and/or aggregate information in accordance with Inscyte's policies and procedures regarding the de-identification of personal health information and limits on the aggregation of data. These policies and procedures explicitly prohibit access to and use of personal health information if other information, such as de-identified and/or aggregate information, will serve the identified purpose and prohibit access to or use of more personal health information than is reasonably necessary to meet the identified purpose.

The policies and procedures also prohibit agents from using de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.



Review and Approval Process

Inscyte Corporation's policies and procedures specify that the Privacy Officer is ultimately responsible for reviewing and approving or denying requests for individuals to obtain access to personal health information.

Inscyte's policies and procedures stipulate that access to personal health information shall be granted to an agent of Inscyte Corporation for the purpose of database maintenance and generating follow-up reminders, or to a health care practitioner (physician, nurse practitioner, or midwife) as a user of the online CytoBase for Clinicians service.

The policies and procedures specify that in approving or denying a request for access to personal health information, Inscyte Corporation shall satisfy itself that:

- The individual making the request routinely requires access to and use of personal health information on an ongoing basis or for a specified period for his or her employment, contractual or other responsibilities.

- The purpose for which access to and use of personal health information is requested is permitted by the Act and its regulation.

- The purpose for which access to and use of personal health information is requested cannot reasonably be accomplished without personal health information.

- De-identified and/or aggregate information will not serve the purpose; and

- No more personal health information will be accessed and used than is reasonably necessary to meet the identified purpose.

Furthermore, the policies state that an agent of Inscyte Corporation shall be granted access provided that the individual has executed a *Personal Health Information Confidentiality and Non-Disclosure Agreement*, and that the individual has received privacy and security awareness training. The policies and procedures specify the documentation required and its content and require that this documentation be reviewed by the Privacy Officer prior to granting access, and that the documentation be retained in perpetuity in Inscyte Corporations privacy document archives.

In regards to CytoBase for Clinicians, the policies specify a formal application process to be followed that requires healthcare practitioners to fill out a standard application form describing the applicant's identity, contact information, and place of work; providing his/her related professional license number; and providing photographic ID. The approval process requires

verification of the person's identity and standing with his/her applicable licensing body. The Privacy Officer is responsible for reviewing and approving/denying applications. Users of the CytoBase for Clinicians online application must renew their applications on an annual basis.

The policy and procedures also state that decisions approving or denying the request for access to and use of personal health information and the reasons for the decisions are documented and retained in Inscyte's privacy document archives; provide the format for the documentation and methods of communication; specify that all decisions shall be communicated to the Privacy Officer and to the individual applying for access; and that the Privacy Officer is responsible for ensuring that all documentation is kept up-to-date and accurate.

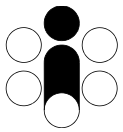
Conditions or Restrictions on the Approval

Inscyte's policies and procedures stipulate that access to personal health information shall be granted to an agent of Inscyte Corporation for the purpose of database maintenance and generating follow-up reminders, or to a health care practitioner (physician, nurse practitioner, or midwife) as a user of the online CytoBase for Clinicians service.

Those agents of Inscyte Corporation who are granted access to personal health information are permitted to read, create, update or delete personal health information in accordance with procedures governing these actions, which require documented instructions from source laboratories in to modify personal health information. The policies state that agents of Inscyte Corporation cannot modify personal health information without express written instructions from the source(s) of these data. Inscyte's policy states that agent access rights remain in effect for the duration of a person's employment although access rights may be terminated earlier at the direction of the Privacy Officer, or in the event that an individual is found to be in breach of privacy or security.

Users of the CytoBase for Clinicians service are only granted the ability to read personal health information. As part of the application process, these individuals also agree to only retrieve and review information on persons within their care, and not to browse the database. Inscyte's policies state that individual access to CytoBase for Clinicians online service expires on an annual basis and requires renewal in accordance with the application process.

Inscyte's policies and procedures also state that an agent of Inscyte shall not access or use personal health information except as necessary for his or her employment, contractual or other responsibilities; and shall not access or use personal health information if other information will serve the identified purpose; and shall not access and use more personal health information than is reasonably necessary to meet the identified purpose. Inscyte also ensures that all accesses to and uses of personal health information are permitted by the Act and its regulation.



Inscyte's policies and procedures also restrict its agents and users of CytoBase for Clinicians from disclosure of personal health information to other parties and stipulate that the use and disclosure of the personal health information must be permitted by the Act and its regulation.

Notification and Termination of Access and Use

Inscyte policies require that Inscyte be notified in writing when an agent has had his/her access rights to CytoBase terminated and stipulate that the notification must contain the name of the individual, his/her position, the date and the reason for the termination. The policies state that it is the responsibility of the Security Officer to inform the Privacy Officer of the termination and to ensure that the termination event is documented in the *Log of Individuals Having Access to PHI*. The policies identify the agent(s) to whom notification must be made and stipulate a time frame of five business days within which to make the notification of termination. A summary report of recent changes to staff having access to CytoBase is also prepared by Inspirata and presented at Inscyte Board meetings.

Inscyte ensures that the procedures implemented in regard of terminating agent access rights to CytoBase are in accordance with its policies and procedures concerning Termination or Cessation of Employment or Contractual Relationship. It is the responsibility of the Security Officer to ensure that access keys and access cards to secure premises are returned, and that computer access accounts are revoked, within one business day of termination of access or cessation of employment or contract of agents who are not healthcare providers.

Inscyte Corporation also requires that its Agent, Inspirata inform Inscyte about changes to the roster of healthcare practitioners having access to the CytoBase for Clinicians online service. This information is communicated to Inscyte's Privacy Officer by Inspirata's Security Officer at the time a change occurs and is documented in the CytoBase for Clinicians User Account Log. A summary report of recent changes to the roster is prepared by the Privacy Officer and presented at Inscyte Board meetings.

Secure Retention

Inscyte's policy and procedures require that agents of Inscyte granted approval to access and use personal health information to securely retain the records of personal health information in compliance with Inscyte's Policies and Procedures for the Secure Retention of Records of Personal Health Information.

Secure Disposal

Inscyte's policy and procedures require that agents of Inscyte granted approval to access and use personal health information to securely dispose of the records of personal health information in compliance with Inscyte's Policy and Procedures for Secure Disposal of Records of Personal Health Information.

Tracking Approved Access to and Use of Personal Health Information

Inscyte policies and procedures stipulate that access to and use of personal health information by individuals is to be tracked in a Log of Individuals Having Access to PHI, as well as a Log of Accounts for CytoBase for Clinicians. It is the responsibility of the Privacy Officer to ensure that these logs are maintained up-to-date and accurate. The policies further specify that these logs shall be retained in perpetuity in Inscyte's privacy documentation archives and that its Agent Inspirata is responsible for maintaining the archives.

Compliance, Audit and Enforcement

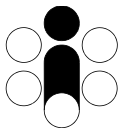
Inscyte Corporation requires that its agents comply with Inscyte's policies and procedures. To enforce compliance, regular privacy and security audits are carried out at the direction of the Privacy Officer, at minimum on an annual basis, an in accordance with Inscyte's policies and procedures with respect to privacy and security audits. The privacy policies and procedures further set out the consequences of breach.

The purpose of the privacy and security audits is to ensure that agents of Inscyte granted access to and use of personal health information continue to be employed or retained by Inscyte or its agent Inspirata, and continue to require access to the same amount and type of personal health information. The policies and procedures state that it is the responsibility of the Privacy Officer to ensure that regular privacy and security audits are conducted. The policies state that privacy audits shall be conducted at minimum on an annual basis, and that security audits shall be conducted on a monthly basis.

Inscyte's policies and procedures require that agents of Inscyte be vigilant of breaches, and report breaches or suspected breaches of privacy to the Privacy Officer at the first reasonable opportunity, in accordance with Inscyte's policies and procedures for privacy/security breach management.

9. Log of Agents Granted Approval to Access and Use Personal Health Information

Inscyte Corporation maintains a Log of Individuals Having Access to PHI, as well as a Log of Accounts for CytoBase for Clinicians, granted approval to access and use personal health information. The log includes the name of each individual granted approval to access and use personal health information; the data holdings of personal health information to which the individual has been granted approval to access and use; the level or type of access and use granted; the date that access and use was granted; and the termination date (or the date of the next audit) of access to and use of the personal health information.



10. Policy and Procedures for the Use of Personal Health Information for Research

Inscyte Corporation's privacy and security policies and procedures state that personal health information in the custody of Inscyte Corporation shall not be disclosed or used to conduct research or support research on individuals or groups of individuals. As such, Inscyte does not accept requests from researchers or research organizations to access and use personal health information for research purposes and does not have policies and procedures in place to manage such requests.

11. Log of Approved Uses of Personal Health Information for Research

Inscyte Corporation's privacy and security policies and procedures state that personal health information in the custody of Inscyte Corporation shall not be disclosed or used to conduct research or support research on individuals or groups of individuals. As such, Inscyte does not maintain a log of approved uses of personal health information for research purposes.

12. Policy and Procedures for Disclosure of Personal Health Information for Purposes Other Than Research

Inscyte's Privacy Policy identifies the purposes for which personal health information is disclosed for purposes other than research, the organizations to whom information can be disclosed, and the requirements that must be satisfied prior to such disclosures. The policies and procedures governing the disclosure of personal health information articulate a commitment by Inscyte Corporation not to disclose personal health information if other information will serve the purpose and not to disclose more personal health information than is reasonably necessary to meet the purpose.

Inscyte Corporation discloses personal health information to its participating laboratories and requires that these laboratories execute a formal Data Sharing Agreement prior to the disclosure of personal health information. Inscyte discloses personal health information to Ontario Health (a prescribed entity under the Act in respect of the Ontario Cervical Cancer Screening Program), and individual Ontario health information custodians (clinicians). Inscyte requires that Ontario Health execute a formal Data Sharing Agreement with Inscyte prior to the disclosure of personal health information. Individual health information custodians are required to execute access agreements for use of the CytoBase for Clinicians online service. In these agreements, Inscyte requires the parties to comply with its policies and procedures and to comply with the requirements of the Act. These agreements also describe how and by whom compliance will be enforced and the consequences of breach. Inscyte Corporation requires its Agents to comply with its policies and procedures in respect of disclosure of personal health information.

The parties to whom Inscyte discloses personal health information are either health information custodians or prescribed persons/entities under the Act. As such, the party executing a Data Sharing Agreement with Inscyte must also comply with the provisions and requirements of the Act. For this reason, Inscyte does not have policies or procedures in place to audit or verify a party's compliance with Inscyte's privacy policies and procedures, as the party's own policies and procedures and obligations under the Act take precedence.

The terms and conditions of Inscyte's Data Sharing Agreements with parties to whom it discloses personal health information require that the parties notify Inscyte Corporation, at the first reasonable opportunity, if the party breaches or believes there may have been a breach of privacy in respect of personal health information disclosed to the party by Inscyte Corporation.

Where the Disclosure of Personal Health Information is Permitted

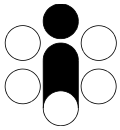
Inscyte Corporation's policies and procedures set out the purposes and the circumstances under which the disclosure of personal health information is permitted. The policies and procedures further require that all disclosures of personal health information comply with the Act and its regulation.

Review and Approval Process

Inscyte's policies and procedures identify the personnel responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of personal health information for purposes other than research, and the process that must be followed in this regard, including a description of the documentation that must be completed, provided and/or executed.

The policies require that organizations to whom Inscyte discloses personal health information execute a formal Data Sharing agreement with Inscyte Corporation prior to the disclosure taking place. The President of Inscyte is responsible for executing the data sharing agreements. The President of Inscyte is responsible for determining whether to approve or deny any request for the disclosure of personal health information for purposes other than research for ensuring that the disclosure is permitted by the Act and its regulation and that any and all conditions or restrictions set out in the Act and its regulation have been satisfied.

The policies require that individual healthcare providers seeking access to the CytoBase for Clinicians online service fill out and submit Inscyte's standard application form, for review and approval by Inscyte, prior to gaining a personalized access account. The policies require applicants to provide their full name, address and contact information, professional license information, and photographic identification. The policies specify that individual healthcare providers must provide this information to Inscyte in hardcopy format using Inscyte's standard application forms. The policies specify the criteria for granting an individual access to CytoBase for Clinicians as (a) being a licensed healthcare provider in the province of Ontario engaged in



gynecological health, (b) in good standing with his/her licensing authority, (c) providing photographic ID, and (d) agreeing to and signing the terms and conditions of the access agreement, which re-iterates the requirement to maintain patient information private and secure. The policies and procedures also describe the method for verifying personal identity and professional standing. The Privacy Officer is responsible for determining whether to approve or deny any request for access to CytoBase for Clinicians and for ensuring that the disclosure is permitted by the Act and its regulation and that any and all conditions or restrictions set out in the Act and its regulation have been satisfied.

Inscyte's policies state that the minimum criteria for disclosure of personal health information is that the disclosure is permitted under the Act and that any and all conditions or restrictions set out in the Act and its regulation have been satisfied. The policies further require The President of Inscyte and its Privacy Officer to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose of the disclosure and that no more personal health information is being requested than is reasonably necessary to meet the identified purpose.

Inscyte's policies and procedures set out the manner in which decisions approving or denying a request for the disclosure of personal health information for purposes other than research are made, and that the reasons for the decisions are documented. Decisions regarding Data Sharing Agreements are documented in business letters to the organization requesting access to CytoBase information. Decisions regarding applications for access to the CytoBase for Clinicians online service are documented on the application form(s) and communicated to individual applicants. Inscyte maintains copies of all decisions and communications in its privacy document archives.

Conditions or Restrictions on the Approval

Inscyte's policies and procedures identify the conditions or restrictions that are required to be satisfied prior to the disclosure of personal health information for purposes other than research, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or other persons or organizations responsible for completing, providing or executing the documentation and/or agreements. With respect to disclosure of personal health information to an organization, the policy and procedures require a Data Sharing Agreement to be executed in accordance with the Policy and Procedures for the Execution of Data Sharing Agreements and Inscyte's template Data Sharing Agreement prior to any disclosure of personal health information for purposes other than research.

The policy and procedures identify the President of Inscyte as being ultimately responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of personal health information have in fact been satisfied, including the execution of a formal Data Sharing Agreement or the execution of CytoBase for Clinicians Access Agreements.

Secure Transfer

Inscyte's policies and procedures require records of personal health information to be transferred in a secure manner in compliance with its Policy and Procedures for Secure Transfer of Records of Personal Health Information. These policies and procedures set out the minimum acceptable encryption and authentication standards for the secure transfer of personal health information using computing networks, portable media, and mobile devices.

Secure Return or Disposal

Inscyte's policies and procedures stipulate that each Data Sharing Agreement set out the retention period and the appropriate methods of return or destruction of personal health information by the recipient upon the expiry of the retention period in the Data Sharing Agreement or the termination or the Data Sharing Agreement itself. Inscyte's policies and procedures set out acceptable methods and procedures for the secure return or destruction of personal heath information on various digital media, mobile devices and paper records.

The policies further stipulate that recipients of personal healthcare information that are required to return or destroy personal health information upon the expiry of the retention period specified in the Data Sharing Agreement, or the termination of the Data Sharing Agreement itself, shall provide to Inscyte a document of *Confirmation of Return and/or Destruction of Personal Health Information*, describing the information holding, the date of return/destruction, the name and title of the person attesting to the return/destruction, and the method of destruction, within ninety business days of the expiry of the retention period in the Data Sharing Agreement, or the termination of the Data Sharing Agreement. In the event that Inscyte does not receive such confirmation in the allotted time period, it is the responsibility of the Privacy Officer to follow-up with the party to obtain such confirmation. In the event that confirmation of return and/or destruction of personal health information cannot be resolved or verified, the policies require the matter to be escalated to the President of Inscyte for resolution, which may include legal action.

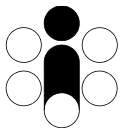
Inscyte Corporation's policy is to retain all *Confirmation of Return and/or Destruction of Personal Health Information* documentation in its privacy document archives in perpetuity.

Documentation Related to Approved Disclosures of Personal Health Information

Inscyte Corporation's privacy policy stipulates that documentation related to the receipt, review, approval or denial of requests for the disclosure of personal health information for purposes other than research will be retained in perpetuity in Inscyte's privacy document archives and that it is the responsibility of the Privacy Officer to ensure compliance with this policy.

Where the Disclosure of Personal Health Information is not Permitted

Inscyte Corporation's privacy policy states that personal health information in its custody shall not be disclosed to any party where the disclosure is not permitted under the Act and expressly



prohibits the disclosure of personal health information for non-research purposes, except where required by law.

Where the disclosure of personal health information is not permitted under the Act, Inscyte's privacy policy permits the disclosure of de-identified or aggregated data should such information be acceptable to the recipient. Under these circumstances the de-identification and/or aggregation of data is performed in accordance with Inscyte's policies and procedures for de-identification and aggregation of personal health information to prevent the inadvertent disclosure of a person's identity resulting from a small number of observations in an aggregation, taking into account the recipient of the information and giving regard to section 4(2) of the Act, which states that information is identifying if it identifies an individual or if it is reasonably foreseeable that the information could be utilized, either alone or with other information, to identify an individual.

Review and Approval Process

Inscyte's policies and procedures identify the Privacy Officer as being responsible for receiving, reviewing, and determining whether to recommend approving or denying a request for the disclosure of de-identified and/or aggregated data. The President of Inscyte is ultimately responsible for authorizing the release of de-identified and/or aggregated data.

Inscyte's policies and procedures set out the requirements that must be satisfied and the criteria that must be considered by the Privacy Officer in determining whether to recommend to approve or deny the request for the disclosure of de-identified and/or aggregate information for purposes other than research. The policies state that the intended use of the de-identified and/or aggregate information must be consistent with the objectives of CytoBase in improving patient care and reducing the burden of cervical cancer. Further the policies require the de-identified and/or aggregate information to be reviewed by the Privacy Officer prior to the disclosure to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual.

Inscyte's policies and procedures require the requester to provide a written *Letter of Request* to the Privacy Officer describing the requester's identity, the scope of de-identified or aggregated information required, and the purpose and/or intended use of this information. The Privacy Officer is responsible for reviewing and qualifying the request using the stated criteria and communicating with the requester during the review process. The President of Inscyte is ultimately responsible for authorizing the release of the de-identified and/or aggregated data. The approval is documented in a *Letter of Authorization* sent to the requester and copied to the Privacy Officer. The Letter of Authorization must also be signed by the receiving party acknowledging and attesting to that the person or organization will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual.

This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

Inscyte's policy is to retain communications and reasons for the decision approving or denying the request for the disclosure of de-identified and/or aggregate information for purposes other than research in its privacy document archives in perpetuity.

Conditions or Restrictions on the Approval

Inscyte's policies and procedures stipulate that the disclosure of de-identified and/or aggregate information for non-research purposes requires:

a) A *Letter of Request* identifying the requester, the scope of information requested and the intended use of the information.

b) A review by the Privacy Officer describing the de-identified and/or aggregated information and the risk of identifying an individual if it is reasonably foreseeable that the information could be utilized, either alone or with other information, to identify an individual; and

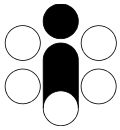
c) A *Letter of Authorization* from the President of Inscyte approving the disclosure.

d) Signed written acknowledgement from the recipient that it will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

Inscyte's policies and procedures identify the Privacy Officer as being responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of the de-identified and/or aggregate information have in fact been satisfied, including the execution of the written acknowledgement. Further, the policies and procedures require that the Privacy Officer track receipt of the executed written acknowledgments and retain these in perpetuity in Inscyte's privacy document archives.

13. Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements

Inscyte Corporation's privacy and security policies and procedures state that personal health information in the custody of Inscyte Corporation shall not be disclosed or used to conduct research or support research on individuals or groups of individuals. As such, Inscyte does not accept requests from researchers or research organizations to access and use personal health



information for research purposes and does not have policies and procedures in place to manage such requests or execute such requests.

14. Template Research Agreement

Inscyte Corporation's privacy and security policies and procedures state that personal health information in the custody of Inscyte Corporation shall not disclosed or used to conduct research or support research on individuals or groups of individuals. As such, Inscyte does not maintain template research agreements.

15. Log of Research Agreements

Inscyte Corporation's privacy and security policies and procedures state that personal health information in the custody of Inscyte Corporation shall not disclosed or used to conduct research or support research on individuals or groups of individuals. As such, Inscyte does not maintain a log of research agreements.

16. Policy and Procedures for the Execution of Data Sharing Agreements

Inscyte's privacy policies and procedures require Data Sharing Agreements to be executed between Inscyte and third parties under any circumstance that involves either the collection and/or disclosure of personal health information between the parties, before the collection and/or disclosure of personal health information taking place. The policies and procedures further specify that Data Sharing Agreements may only be executed with parties that are legally permitted to exchange personal health information with Inscyte. In practice this restricts the parties that may enter into a Data Sharing Agreement for the collection/disclosure of personal health information with Inscyte Corporation to Ontario health information custodians and prescribed persons/entities under the Act.

The only exception to the requirements for executing a Data Sharing Agreement is the disclosure of personal health information to individual healthcare providers in Ontario via the CytoBase for Clinicians online service, which requires individually signed Access Agreements to be executed between Inscyte and individual providers in place of a Data Sharing Agreement.

The policies and procedures describe the process for executing Data Sharing Agreements and the required content, terms and conditions of these agreements. The policies require that each Data Sharing Agreement describe the purpose for the collection/disclosure; that the purpose is consistent with the objectives and intended use of CytoBase; that the agreement describe the precautions to be taken to secure the information during exchange; the precautions to be taken to secure the storage of the information; the limitations on retention of the information; and the requirements for secure return or destruction of the information. The policies also stipulate that Data Sharing Agreements require each party to inform the other, at the first reasonable opportunity, if the party believes a breach of privacy has occurred or may occur.

The policies further specify that it is the responsibility of the President of Inscyte to execute Data Sharing Agreements with third parties prior to the collection/disclosure of personal health information and to ensure that all requirements of Data Sharing Agreements are satisfied, taking into account the approval processes in respect of the policies and procedures for disclosure of personal health information for purposes other than research and/or the policies and procedures for the collection of personal health information.

Inscyte's policies and procedures also require that all executed Data Sharing Agreements are retained in a perpetual Log of Data Sharing Agreement within its privacy document archives. This includes copies of executed and signed agreements. The policies state that it is the responsibility of the Privacy Officer to ensure that the Log of Data Sharing Agreements is maintained up-to-date and complete.

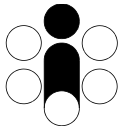
The parties to Inscyte's Data Sharing Agreements are either health information custodians or prescribed persons/entities under the Act. As such, the party executing a Data Sharing Agreement with Inscyte must also comply with the provisions and requirements of the Act. For this reason, Inscyte does not have policies or procedures in place to audit or verify a party's compliance with Inscyte's privacy policies and procedures, as the party's own policies and procedures and obligations under the Act take precedence.

Inscyte Corporation requires its agents to comply with this policy and its procedures and designates the Privacy Officer as being responsible for enforcing compliance. Inscyte's policies and procedures set out the consequences of breach and stipulate that compliance will be audited on an annual basis at minimum, in accordance with Inscyte's the Policy and Procedures in Respect of Privacy Audits, and designate the Privacy Officer as being responsible for conducting the audits and for ensuring compliance with the policy and its procedures.

Inscyte's policy and procedures require its agents to notify Inscyte at the first reasonable opportunity, in accordance with the Policy and Procedures for Privacy Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.

17. Template Data Sharing Agreement

Inscyte Corporation ensures that a Data Sharing Agreement is executed in the circumstances set out in the Policy and Procedures for the Execution of Data Sharing Agreements. Inscyte's policies and procedures require that a Template Data Sharing Agreement be kept on file and that all Data Sharing Agreements address the following.



General Provisions

Inscyte's template Data Sharing Agreement describes the status of Inscyte Corporation with respect to CytoBase under the Act and the duties and responsibilities arising from this status. The template agreement provides a definition of personal health information consistent with the Act and its regulation and provides for specifying the precise nature of the personal health information subject to the Data Sharing Agreement. The template Data Sharing Agreement provides for identifying the organization that is collecting personal health information and the organization that is disclosing personal health information pursuant to the agreement.

Purposes of Collection, Use and Disclosure

Inscyte's template Data Sharing Agreement identifies the purposes for which the personal health information subject to the Data Sharing Agreement is being collected and for which the personal health information will be used. The Data Sharing Agreements explicitly state whether or not the personal health information collected pursuant to the Data Sharing Agreement will be linked to other information, and if so, the Data Sharing Agreement identifies the nature of the information to which the personal health information will be linked, the source of the information to which the personal health information will be linked, how the linkage will be conducted and why the linkage is required for the identified purposes.

The template Data Sharing Agreement includes an acknowledgement that the personal health information collected pursuant to the Data Sharing Agreement is necessary for the purpose for which it was collected and that other information, namely de-identified and/or aggregate information, will not serve the purpose and that no more personal health information is being collected and will be used than is reasonably necessary to meet the purpose.

The template Data Sharing Agreement also identifies the purposes, if any, for which the personal health information subject to the Data Sharing Agreement may be disclosed and any limitations, conditions or restrictions imposed thereon.

The template Data Sharing Agreement requires the collection, use and disclosure of personal health information subject to the Data Sharing Agreement to comply with the Act and its regulation and sets out the specific statutory authority for each collection, use and disclosure contemplated in the Data Sharing Agreement.

Secure Transfer

Inscyte's template Data Sharing Agreement requires the secure transfer of the records of personal health information subject to the Data Sharing Agreement. The Data Sharing Agreement sets out the secure manner in which the records of personal health information will be transferred, including under what conditions and to whom the records will be transferred, and the procedure that will be followed in ensuring that the records are transferred in a secure

manner. Inscyte's policies and procedures prescribe acceptable methods for the secure transfer of personal health information in various formats and media.

Secure Retention

Inscyte's template Data Sharing Agreement addresses the retention period of personal health information to ensure that the information is retained only for as long as required to fulfill the purpose for which personal health information is collected.

The template Data Sharing Agreement requires that records of personal health information are stored in a secure manner consistent with Inscyte's policies and procedures for the secure storage of personal health information in various formats and media, which address steps to be taken to ensure that the personal health information subject to the Data Sharing Agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information are protected against unauthorized copying, modification or disposal.

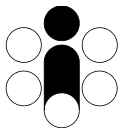
Each instance of a Data Sharing Agreement describes the secure manner in which personal health information will be stored by the parties to the agreement and the steps to be taken to protect the information against theft, loss, unauthorized use or disclosure, copying, modification and disposal.

Secure Return or Disposal

Inscyte's template Data Sharing Agreement also addresses whether the records of personal health information subject to the Data Sharing Agreement will be returned in a secure manner or will be disposed of in a secure manner following the retention period set out in the Data Sharing Agreement or following the date of termination of the Data Sharing Agreement, as the case may be.

If the records of personal health information are required to be returned in a secure manner, the Data Sharing Agreement specifies the time frame following the retention period, or the date of termination of the agreement, within which the records of personal health information must be securely returned, that the records should be returned to the Privacy Officer of Inscyte, and the manner of secure return consistent with Inscyte's policies and procedures for the secure transfer of personal health information.

If the records of personal health information are required to be disposed of in a secure manner, the Data Sharing Agreement specifies the time frame following the retention period, or the date of termination of the agreement, within which the records of personal health information must be securely destroyed and a Certificate of Destruction to be sent to the Privacy Officer of Inscyte attesting to the destruction of the records. The Certificate of Destruction must include at minimum: a description of the record set that was destroyed, the date and time the records were



destroyed, the location where the records were destroyed, the method by which the records were destroyed, the name of the person who destroyed the records, and the name and signature of the person attesting to the destruction of the records.

If the records of personal health information are required to be disposed of in a secure manner, the Data Sharing Agreement further describes acceptable methods of destruction, consistent with Inscyte's Policies and Procedures for the Secure Disposal of Personal Health Information in various formats and media, which are consistent with the Act and its regulations, and give regard to orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation, including Fact Sheet 10: Secure Destruction of Personal Information.

Notification

Inscyte's template Data Sharing Agreement requires that notification be provided at the first reasonable opportunity if the Data Sharing Agreement has been breached or is suspected to have been breached or if the personal health information subject to the Data Sharing Agreement is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons. Inscyte's policies regarding breach management require the notification to be made in writing to the Privacy Officer of Inscyte, and set out the steps to be taken to contain the breach, including containing the breach of the Data Sharing Agreement and contain the theft, loss or access to PHI by unauthorized persons

Consequences of Breach and Monitoring Compliance

The parties to Inscyte's Data Sharing Agreements are either health information custodians or prescribed persons/entities under the Act and must therefore also comply with the provisions and requirements of the Act. For this reason, Inscyte's Data Sharing Agreements do not include provisions for monitoring and auditing compliance of the other party. Instead, the template Data Sharing Agreement stipulates that each party must agree to monitor compliance with the terms and conditions of the data Sharing Agreement in accordance with its own policies and procedures regarding privacy and/or security audits, breach management, containment, and the consequences of breach. Similarly, Inscyte's template Data Sharing Agreements do not require that individual persons who will be given access to personal health information sign an acknowledgment with Inscyte, as these persons will be required to sign confidentiality and non-disclosure agreements with the healthcare custodian or prescribed person/entity that is party to the Data Sharing Agreement.

18. Log of Data Sharing Agreements

Inscyte Corporation maintains a log of executed Data Sharing Agreements, which includes:

1. The name of the organization from which the personal health information is (was) collected and/or to which the personal health information is (was) disclosed.

2. The date that the collection or disclosure of personal health information was approved, as the case may be.

3. The date that the Data Sharing Agreement was executed.

4. The date the personal health information was collected or disclosed, as the case may be.

5. The nature of the personal health information subject to the Data Sharing Agreement.

6. The retention period for the records of personal health information set out in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement.

7. Whether the records of personal health information will be securely returned or will be securely disposed of following the retention period set out in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement; and

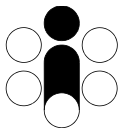
8. The date the records of personal health information were securely returned, or a certificate of destruction was provided or the date by which they must be returned or disposed of.

19. Policy and Procedures for Executing Agreements with Third-Party Service Providers in Respect of Personal Health Information

Inscyte's policies require a written agreement to be entered into with third party service providers whenever such services entail access to, or use of personal health information, prior to permitting third party service providers to access and use the personal health information. The policies and procedures require the written agreements to contain the relevant language from Inscyte's Template Agreement for Third Party Service Providers.

The policies and procedures state that the President of Inscyte is responsible for ensuring that a Third-Party Service Agreement is executed in all cases where such services involve access to or use of personal health information. This policy does not apply to third party services where access to or use of personal health information is not required.

The policy and procedures specify that Inscyte shall not provide personal health information to a third-party service provider if other information, namely de-identified and/or aggregate information, will serve the purpose and will not provide more personal health information than



is reasonably necessary to meet the purpose. The Privacy Officer of Inscyte is responsible for making this determination.

The policy and procedures specify that the Privacy Officer is responsible for ensuring that records of personal health information provided to a third-party service provider are either securely returned or are securely disposed of, as the case may be, following the termination of the agreement. In the event that records of personal health information are not returned or a confirmation of destruction of the records is not received within the time frame stipulated in the Third-Party Service Agreement, it is the responsibility of the Privacy Officer of Inscyte to inform the third party in writing that failure to return or destroy the records in accordance with the terms and conditions of the agreement constitutes a breach of the agreement. If the third party fails to comply after such notification, the matter is escalated to the President of Inscyte, and if compliance is not achieved may result in legal action.

Inscyte's policy requires that a log be maintained of all agreements executed with third party service providers and designates the Privacy Officer as responsible for maintaining the Log of Third Party Service Agreements in Inscyte's privacy document archives, including signed copies of all executed agreements.

The terms and conditions of Inscyte's Third Party Service Agreements require the third party and Agents to comply with Inscyte's privacy and security policies and procedures and designate the Privacy Officer of Inscyte as being responsible for monitoring and auditing third party compliance. Compliance will be audited in accordance with Inscyte's policies and procedures in respect of privacy audits, at a frequency specified and agreed to in the Third-Party Service Agreement. Inscyte Corporation may conduct the audit or designate its Agent, Inspirata, to perform the audit as required.

The terms and conditions of Inscyte's Third Party Service Agreements require the third party and Agents to notify Inscyte, at the first reasonable opportunity, if the third-party breaches or believes there may have been a breach of privacy and security as defined in Inscyte's policies and procedures and to comply with Inscyte's breach management policies and procedures.

20. Template Agreement for All Third-Party Service Providers

Inscyte Corporation maintains a template Third Party Service Agreement to be used with third party services providers whenever the third party will be given access to, or use of, Inscyte's holdings of personal health information in the course of carrying out the work under the service agreement, including those that are contracted to retain, transfer or dispose of records of personal health information.

The template Third Party Service Agreement applies to third party service providers who are not agents of Inscyte and where access to personal health information is required to fulfill the third party's service agreement.

The template Third Party Service Agreement does not apply to third party service providers who work peripherally with equipment that facilitates the means to collect, use, modify, disclose, or retain personal health information, such as hardware/software vendors, equipment maintenance contractors, Internet service providers, facility maintenance services, etc., where access to personal health information is not required to fulfill the third party's service agreement.

Inscyte's template Third Party Service Agreement addresses the matters set out below.

General Provisions

The template Third Party Service Agreement describes the status of Inscyte Corporation under the Act and the duties and responsibilities arising from this status. The agreement also identifies whether or not the third-party service provider is an agent of Inscyte in providing the services. All third-party service providers that are permitted to access and use personal health information in the course of providing services to Inscyte are considered agents of Inscyte.

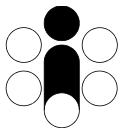
In the event that a third-party service provider is an agent of Inscyte, the agreement requires the third-party service provider to comply with the provisions of the Act and its regulation, and to comply with Inscyte's privacy and security policies in providing services pursuant to the agreement.

Inscyte's template Third Party Service Agreement includes a definition of personal health information that is consistent with the Act and its regulation. The agreement also specifies the precise nature of the personal health information that the third-party service provider will be permitted to access and use while providing services pursuant to the agreement.

Inscyte's template Third Party Service Agreement also requires that the services provided by the third-party service provider be performed in a professional manner, in accordance with industry standards and practices, and by properly trained staff of the third-party service provider.

Obligations with Respect to Access and Use

Inscyte's template Third Party Service Agreement identifies the purposes for which the third-party service provider is permitted to access and use the personal health information of the prescribed person or prescribed entity and any limitations, conditions or restrictions imposed thereon. Inscyte further ensures that each use identified in the agreement is consistent with the uses of personal health information permitted by the Act and its regulation. The agreement explicitly prohibits the third-party service provider from using personal health information except as permitted in the agreement.



The template Third Party Service Agreement also prohibits the third-party service provider from using personal health information if other information will serve the purpose and from using more personal health information than is reasonably necessary to meet the purpose.

Obligations with Respect to Disclosure

The template Third Party Services Agreement identifies the purposes, if applicable, for which the third-party service provider is permitted to disclose the personal health information and the limitations, conditions or restrictions imposed on the disclosure. Specifically, the agreement states that such disclosure must be consistent with the Act and its regulations and comply with Inscyte's policies and procedures for the disclosure of personal health information. The agreement further prohibits the third party from disclosing personal health information except as permitted in the agreement or as required by law, from disclosing personal health information if other information will serve the purpose and, from disclosing more personal health information than is reasonably necessary to meet the purpose.

Secure Transfer

In the event that a Third-Party Services Agreement contemplates the transfer of personal health information between Inscyte and another party, the agreement requires that such transfer of personal health information comply with Inscyte's policies and procedures for the secure transfer of personal health information in various formats and media. Specifically, the agreement sets out the secure manner in which the records will be transferred by the third-party service provider, the conditions under which the records will be transferred, to whom the records will be transferred, and the procedures that must be followed by the third-party service provider in ensuring that the records are transferred in a secure manner.

In addition, where the retention of records of personal health information or where the disposal of records of personal health information outside the premises of Inscyte is the primary service provided to Inscyte, the agreement requires the third party service provider to provide documentation to Inscyte setting out the date, time and mode of transfer of the records of personal health information and confirming receipt of the records of personal health information by the third party service provider. In these circumstances, the agreement obligates the third-party service provider to maintain a detailed inventory of the records of personal health information transferred.

Secure Retention

In the event that a Third-Party Services Agreement contemplates the retention of personal health information by an agent of Inscyte, the agreement requires that the retention comply with Inscyte's policies and procedures regarding the secure storage and retention of personal health

information in various formats and media, and describes the responsibilities of the service provider in securely retaining the records of personal health information.

Where the retention of records of personal health information is the primary service provided to Inscyte by the third party service provider, the agreement obligates the third party service provider to maintain a detailed inventory of the records of personal health information being retained on behalf of Inscyte as well as the methods used to track the records being retained.

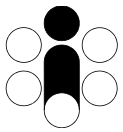
Secure Return or Disposal Following Termination of the Agreement

Inscyte's template Third Party Services Agreement addresses, where applicable, whether records of personal health information will be securely returned to Inscyte or will be disposed of in a secure manner following the termination of the agreement.

In the event that records of personal health information are to be returned to Inscyte the agreement specifies that the records are to be returned to the Privacy Officer of Inscyte, the format and/or media in which the records are to be returned, the time frame following the date of termination of the agreement within which the records must be returned, that the method of returning the records in compliance with Inscyte's policies and procedures regarding the secure transfer of personal health information in various formats and media.

If the event that records of personal health information are to be disposed of in a secure manner, the agreement describes acceptable methods of destruction, consistent with Inscyte's policies and procedures for the secure destruction of personal health information in various formats and media, which are consistent with the Act and its regulations, and give regard to orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation, including Fact Sheet 10: Secure Destruction of Personal Information.

If the records of personal health information are required to be disposed of in a secure manner, the agreement specifies the time frame following the termination of the agreement, within which the records of personal health information must be securely destroyed and a Certificate of Destruction to be sent to the Privacy Officer of Inscyte attesting to the destruction of the records. The Certificate of Destruction must include at minimum: a description of the record set that was destroyed, the date and time the records were destroyed, the location where records were destroyed, the method by which the records were destroyed, the name of the person who destroyed the records, and the name and signature of the person attesting to the destruction of the records.



Secure Disposal as a Contracted Service

In circumstances where the disposal of records of personal health information is the primary service provided to Inscyte or its agents by the third party service provider, in addition to the requirements above in relation to secure disposal, the agreement sets out the responsibilities of the third party service provider in securely disposing of the records of personal health information, including:

- The time frame within which the records are required to be securely disposed of.
- The precise method by which records in paper and/or electronic format must be securely disposed of, including records retained on various media.
- The conditions pursuant to which the records will be securely disposed of; and
- The person(s) responsible for ensuring the secure disposal of the records.

The agreement also enables Inscyte, at its sole discretion, to witness the secure disposal of the records of personal health information subject to such reasonable terms or conditions as may be required in the circumstances.

Implementation of Safeguards

Inscyte's template Third Party Services Agreement details the precautions and safeguards that a service provider is required to implement to ensure that personal health information accessed and used in the course of providing services is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information subject to the agreement are protected against unauthorized copying, modification or disposal. The agreement states that these precautions must be consistent with Inscyte's policies and procedures for the secure storage, transfer and/or destruction of personal health information in various formats and media.

Training of Agents of the Third Party Service Provider

Inscyte's template Third Party Services Agreement requires that a service provider who is an agent of Inscyte must provide training to its staff regarding the importance of protecting the privacy of individuals whose personal health information is accessed and used in the course of providing services pursuant to the agreement and on the consequences that may arise in the event of a breach of these obligations.

The agreement further requires the service provider to ensure that its agents who will have access to the records of personal health information are aware of and agree to comply with the terms and conditions of the agreement prior to being given access to the personal health information. To this end, the agreement requires agents to sign an acknowledgement, prior to being granted access to the personal health information, indicating that they are aware of and agree to comply with the terms and conditions of the agreement.

Subcontracting of the Services

In the event that the Third Party Services agreement permits an agent of Inscyte to subcontract certain services to be provided under the agreement, the agreement requires the agent to acknowledge and agree that it will provide Inscyte with advance notice of its intention to do so, that agent will enter into a written agreement with the subcontractor on terms consistent with its obligations to Inscyte, and that a copy of the sub-contract agreement will be provided to Inscyte.

Notification

Inscyte's template Third Party Services Agreement requires the third party service provider to notify Inscyte at the first reasonable opportunity if there has been a breach or suspected breach of the agreement or if personal health information handled by the third party service provider on behalf of Inscyte is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons. The agreement requires that the notification be made to the Privacy Officer of Inscyte, both verbally and in writing, and that under such circumstances Inscyte's policies and procedures for breach management shall come into force.

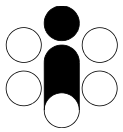
Consequences of Breach and Monitoring Compliance

The Third Party Services Agreement indicates that Inscyte may, at any time and at its sole discretion, conduct a review/audit of the practices of the third party service provider to ensure it is in compliance with Inscyte's privacy and security policies and procedures as described in the agreement. In the event that Inscyte wishes to conduct an audit, it notifies the third party service provider of its intent in writing. The Third Party Services Agreement also describes the consequences of breach of the agreement.

21. Log of Agreements with Third Party Service Providers

Inscyte maintains a perpetual log of executed agreements with third party service providers in its privacy document archives, which includes:

- The name of the third party service provider;
- The nature of the services provided by the third party service provider that require access to and use of personal health information;
- The date that the agreement with the third party service provider was executed;
- The date that the records of personal health information or access to the records of personal health information, if any, was provided.
- The nature of the personal health information provided or to which access was provided.
- The date of termination of the agreement with the third party service provider;
- Whether the records of personal health information, if any, will be securely returned or will be securely disposed of following the date of termination of the agreement; and



- The date the records of personal health information were securely returned or a certificate of destruction was provided or the date that access to the personal health information was terminated or the date by which the records of personal health information must be returned or disposed of or access terminated.

22. Policy and Procedures for the Linkage of Records of Personal Health Information

Inscyte's privacy policy permits linkage of data with external sources provided that the that the linkage is permitted under law, that the purpose of the linkage is consistent with the purpose of CytoBase, and that the other party has executed a Data Sharing Agreement with Inscyte prior to the linkage taking place. Further, the policies state that if the linkage results in a disclosure of personal health information by Inscyte to another person or organization, the linkage is permitted only if the other party is a healthcare custodian or a prescribed entity/person under the Act and its regulations.

Review and Approval Process

Inscyte's policies and procedures stipulate that requests for data linkages must be addressed to the President of Inscyte and designate the President of Inscyte as being ultimately responsible for reviewing requests and approving/denying requests for data linkage. The request procedure requires that requests be submitted in writing to the President of Inscyte describing the purpose of the linkage, the nature of the data elements to be linked and the data elements that will be disclosed by each party to the other as a result of the linkage.

The policy and procedures designate the President of Inscyte as being responsible for reviewing and approving or denying requests for data linkage with CytoBase. The policies state that the minimum criteria used for evaluating requests for data linkage are:

a) The linkage must be permitted by law, and
b) The purpose of the linkage must be consistent with Inscyte's policies regarding the collection and use of personal health information, and the general objectives of CytoBase with respect to improving patient care in Ontario.

The policies and procedures require that the decision to approve or deny a request for data linkage be provided by the President of Inscyte to the requesting party in writing, including a documentation of the reason for the decision.

If a request for data linkage is approved, the policies and procedures require that a Data Sharing Agreement be prepared in compliance with Inscyte's policies and procedures in respect of data sharing agreements, and that the Data Sharing Agreement set out the purpose of the linkage, the

frequency of the linkage, the nature of data to be linked and disclosed, the retention periods for linked data, and the disposal requirements for the linked data.

Conditions or Restrictions on Approval

In the event that linked records of personal health information will be disclosed by Inscyte to another person or organization, the policies and procedures require that the disclosure be approved pursuant to Inscyte's Policies and Procedures for the Disclosure of Personal Health Information For Purposes Other Than Research, and the execution of Data Sharing Agreements.

In the event that the linked records of personal health information will be used by Inscyte Corporation, Inscyte's policies and procedures require that the use be approved pursuant to Inscyte's Policy and Procedures for the Use of Personal Health Information and limiting access to personal health information. Further, Inscyte's policies and procedures state that the linked records of personal health information will be retained only for as long as required to fulfill the purpose of the linkage, and that thereafter, as soon as practicable, the linked data will be de-identified/aggregated or destroyed in compliance with Inscyte's policies for the de-identification/aggregation or destruction of personal health information, as the case may be.

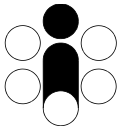
Process for the Linkage of Personal Health Information

Inscyte's policies and procedures in respect of data linkages do not set out any specific process for performing data linkages as these processes may differ depending on the type of data linkage being performed, the frequency of the data linkage, and the desired formats/media of the input and output datasets. The agent(s) responsible for implementing specific processes and performing the data linkage are identified in the Data Sharing Agreement governing the linkage.

The only linkages performed to date are the matching of patient identifying information provided to Inscyte by P-Prompt (which represents healthcare practitioners) with records in CytoBase to determine the most recent cervical cancer screening test date for each patient. The information disclosed by Inscyte is the most recent screening date. Inscyte is permitted to disclose this personal health information to P-Prompt on behalf of health information custodians as per section 49(1)(a) of PHIPA.

Retention

Inscyte's policies and procedures require all data linkages to be carried out under a Data Sharing Agreement, which sets out the requirements regarding retention of the linked data by Inscyte and/or the other party, depending on the purpose of the linkage and the intended use of the linked data, and in compliance with Inscyte's Policies and Procedures for Secure Retention of Records of Personal Health Information until they are de-identified and/or aggregated pursuant to the Policy and Procedures with Respect to De-Identification and Aggregation of personal health information.



Secure Disposal

Inscyte's policies and procedures require all data linkages to be carried out under a Data Sharing Agreement, which sets out the requirements regarding disposal of linked personal health information by Inscyte and/or the other party, when it is no longer required to fulfill its intended purpose and use, in compliance with Inscyte's Policies and Procedures for the Secure Disposal of Personal Health Information.

Compliance, Audit and Enforcement

Inscyte's policies and procedures require all data linkages to be carried out under a Data Sharing Agreement and where the linkage would result in a disclosure of personal health information by Inscyte, the other party must be either health information custodians or prescribed persons/entities under the Act and must therefore also comply with the provisions and requirements of the Act. For this reason, Inscyte's Data Sharing Agreements do not include provisions for monitoring and auditing compliance of the other party. Instead, the Data Sharing Agreement stipulates that each party must agree to monitor compliance with the terms and conditions of the Data Sharing Agreement in accordance with its own policies and procedures regarding privacy and/or security audits, breach management, containment, and the consequences of breach. Further, the Data Sharing Agreement requires each party to notify the other at the first reasonable opportunity, in accordance with the Policy and Procedures for Privacy Breach Management, if the party breaches or believes there may have been a breach of the terms and conditions of the Data Sharing Agreement.

Tracking Approved Linkages of Records of Personal Health Information

Inscyte's policies and procedures require that logs be maintained of the linkages of records of personal health information approved by Inscyte and identifies Inspirata as the agent responsible for maintaining these logs. The logs of data linkages contain the name of the requester, the date/time the linkage was performed, the name of the individual performing the linkage and the disposition of the linked record set. In circumstances where approved data linkages are performed by on an on-going basis by automated processes, Inscyte's policies and procedures require that an audit trail be maintained specifying the date and time of each record linkage and its disposition.

23. Log of Approved Linkages of Records of Personal Health Information

Inscyte Corporation maintains a log of linkages of records of personal health information approved by Inscyte. The log includes the name of the person or organization who requested the linkage; the date that the linkage of records of personal health information was approved or denied; and the nature of the records of personal health information linked, the purpose of the linkage, the frequency of the linkage and a copy of (or reference to) the applicable Data Sharing Agreement governing the linkage.

24. Policy and Procedures with Respect to De-Identification and Aggregation

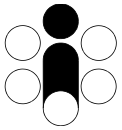
Inscyte's privacy policies and procedures state that personal health information shall not be used or disclosed if other information, namely de-identified and/or aggregate information, will serve the identified purpose. To this end Inscyte has also implemented policies and procedures for the de-identification of personal health information in various formats and media, and policies and procedures setting out the limits on the aggregation of statistical information from personal health information. These policies and procedures provide a definition of personal health information consistent with the Act and its regulations.

Inscyte's policies and procedures define de-identified information as information that cannot be used alone, or in conjunction with other information, under reasonable effort, to identify an individual. The policies and procedures specify that de-identification of personal health information requires outright removal or obfuscation (pseudonym-value substitution) of every element of personal health information as defined in the Act and regulations. The policies state that at minimum the following data elements must be removed or obfuscated in the process of de-identification of personal health information:

a) Patient name, middle name, and last name
b) Patient contact information (address, city, postal code, telephone etc.)
c) Patient health insurance providers/policy numbers
d) Patient medical record numbers and/or chart numbers
e) Patient caregiver names, addresses, contact information
f) Patient date of birth to be converted to "age at" date where possible
g) Specimen accession numbers and/or medical report identifiers
h) Institution, clinic, hospital, laboratory names, addresses, telephone, etc.

Inscyte's policies and procedures specify that encrypted information is not the same as de-identified information because it is subject to decryption. Inscyte's policies and procedures provide examples of acceptable methods of removing and/or obfuscating data to de-identify personal health information in various formats and media, and designate Inspirata as agent responsible for the de-identification and aggregation of information.

Inscyte's policies and procedures define aggregated information as information that contains no patient identifying information whatsoever, but rather represents mathematical counts, ratios, rates, etc. of instances of correlated data. Inscyte's policies stipulate that aggregate information with fewer than five (5) observations per aggregation (cell) is not to be disclosed owing to the elevated risk of potential re-identification due to a low occurrence of instances of the correlated data.



Inscyte Corporation compiles and publishes de-identified aggregated statistics describing trends in cervical cancer screening in Ontario. The aggregation of data is performed in accordance with Inscyte's policies and procedures for de-identification and aggregation of personal health information to prevent the inadvertent disclosure of a person's identity resulting from a small number of observations in an aggregation, taking into account the recipient of the information and giving regard to section 4(2) of the Act, which states that information is identifying if it identifies an individual or if it is reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual.

Inscyte's policies and procedures designate the Privacy Officer of Inscyte as being responsible for the review and approval of the disclosure of de-identified and/or aggregate information and to assess the risk of inadvertent disclosure of a person's identity, taking into account the recipient of the information and the purpose of the disclosure. In making this assessment, the policies and procedures require the Privacy Officer to take section 4(2) of the Act into consideration, which states that information is identifying if it identifies an individual or if it is reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The policies and procedures stipulate that if the risk is deemed inappropriate the information shall not be disclosed.

The process in reviewing the de-identified and/or aggregate information and the criteria used in assessing the risk of re-identification includes verification that no directly identifying information persists in the de-identified and/or aggregate data (e.g., name, address, health card number) and that the de-identified and/or aggregate data does not contain information that could be used, with reasonable effort, and with other information to discover a person's identity (e.g., date-of-birth, postal code, gender) taking into account the resources of the party(ies) to whom the de-identified and/or aggregate data are disclosed. Inscyte's policies and procedures suggest using mathematical tools to quantify the risk (probability) of re-identification of an individual under these circumstances.

Inscyte's policies and procedures prohibit agents of Inscyte from using de-identified and/or aggregate information, including information in cell-sizes of less than five, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

In case that Inscyte were to provide de-identified or aggregated information to a recipient, Inscyte's policies and procedures require that the release of de-identified and/or aggregated information be accompanied by a statement requiring the recipient to acknowledge that the released data will not be used alone or with other information to identify an individual. This statement is provided to the recipient with the released data and requires a signature on behalf of the recipient.

Inscyte requires its agents to comply with its policies and procedures regarding the de-identification and aggregation of personal health information and designates the Privacy Officer as being responsible for monitoring and ensuring compliance. Inscyte's policy and procedures set out the consequences of breach and stipulate that compliance will be audited at minimum on an annual basis, and that spot security audits will be conducted on a monthly basis. The policy states that it is the responsibility of the Privacy Officer to initiate privacy audits and the responsibility of the Security Officer to initiate security audits at the prescribed intervals. The procedures outline the steps involved and the data and documentation holdings that are to be audited and how the results of the audits are to be documented.

Inscyte's policies and procedures require all agents of Inscyte to be vigilant of and notify Inscyte's Privacy Officer, at the first reasonable opportunity, in accordance with the Policy and Procedures for Privacy Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.

25. Privacy Impact Assessment Policy and Procedures

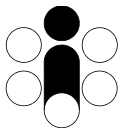
Inscyte Corporation's policy and procedures state that a Privacy Impact Assessments shall be conducted on existing and proposed data holdings involving personal health information whenever a new or a change to an existing information system, technology or program involving personal health information is contemplated. Specifically, the policies and procedures require a Privacy Impact Assessment to be conducted in the event that:

(a) There is a proposed change in the scope or type of personal health information to be collected or a proposed change in the use of the personal health information.
(b) There is a proposed change in the source(s) from which personal health information is collected or to which personal health information is to be disclosed.

The policies also state that Privacy Impact Assessments may not be required in the course of making routine upgrades, repairs, or enhancements to the information and security systems infrastructure, which includes:

(a) Upgrades to supporting software (e.g. O/S version upgrades)
(b) Upgrades/repairs/replacement of hardware (e.g. disk drives, power supplies, routers)
(c) Upgrades to technical security measures (e.g. increasing encryption key strength)
(d) Re-organization of computing infrastructure (e.g. moving to virtual servers, network storage arrays etc.)

The policies state that under the above circumstances, Privacy Impact Assessments are not required provided that the proposed changes will not materially alter or degrade the existing privacy and/or security measures. The policies state that it is the responsibility of the Security



Officer to conduct a risk assessment and advise the Privacy Officer if upgrades and changes to the information system infrastructure could in any way degrade the security measures in place, and that it is the responsibility of the Privacy Officer to review the risk assessments and determine whether or not a Privacy Impact Assessment is required under the circumstances. The policies require the risk assessment and reasons for the determination to be documented in Inscyte's information infrastructure *Asset Inventory* documentation.

The policies state that in the event that new data holdings of personal health information are contemplated or changes to existing information systems, technologies or programs involving personal health information are contemplated, a Privacy Impact Assessment shall be conducted at the conceptual design phase and that the PIA be reviewed and amended, if necessary, during the detailed design and implementation phases. With respect to existing data holdings involving personal health information, the policy and procedures require a timetable to be developed to ensure privacy impact assessments are conducted and designates the Privacy Officer as being responsible for developing the timetable.

Inscyte's policies and procedures require the review of completed Privacy Impact Assessments as part of the annual privacy audit to ensure that the PIAs continue to be accurate and continue to be consistent with the information practices of Inscyte.

The policy and procedures designate the Privacy Officer as being responsible for identifying when privacy impact assessments are required; in identifying when privacy impact assessments are required to be reviewed in accordance with the policy and procedures; in ensuring that privacy impact assessments are conducted and completed; and in ensuring that privacy impact assessments are reviewed and amended, if necessary. The policies designate the Privacy Officer as having been delegated day-to-day authority to manage the privacy program and the Security Officer as having been delegated day-to-day authority to manage the security program in respect of privacy impact assessments.

Inscyte's policy requires the following information, at minimum, to be included in Privacy Impact Assessments:

- The data holding, information system, technology, or program at issue.
- The nature and type of personal health information collected, used or disclosed or that is proposed to be collected, used or disclosed.
- The sources of the personal health information.
- The purposes for which the personal health information is collected, used, or disclosed or is proposed to be collected, used, or disclosed.
- The reason that the personal health information is required for the purposes identified.
- The flows of the personal health information.

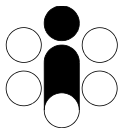
- The statutory authority for each collection, use and disclosure of personal health information identified.
- The limitations imposed on the collection, use and disclosure of the personal health information.
- Whether or not the personal health information is or will be linked to other information.
- The retention period for the records of personal health information.
- The secure manner in which the records of personal health information are or will be retained, transferred and disposed of.
- The functionality for logging access, use, modification and disclosure of the personal health information and the functionality to audit logs for unauthorized use or disclosure.
- The risks to the privacy of individuals whose personal health information is or will be part of the data holding, information system, technology or program and an assessment of the risks.
- Recommendations to address and eliminate or reduce the privacy risks identified; and
- The administrative, technical, and physical safeguards implemented or proposed to be implemented to protect the personal health information.

Inscyte's policies state that, when required, Privacy Impact Assessments are to be conducted and any recommended remedial or corrective actions are to be taken, and that the Privacy Impact Assessment be suitably amended, before the proposed changes that gave rise to the Privacy Impact Assessment are implemented.

Inscyte's policies and procedures designate the Privacy Officer as being responsible for reviewing the recommendations arising from Privacy Impact Assessments, for establishing timelines to address the recommendations and for delegating work to other agents to implement the recommendations, and for monitoring and ensuring that the recommendations are implemented in a timely and effective manner.

Inscyte's policies and procedures state that Privacy Impact Assessments are to be reviewed as part of regular privacy audits, which are to be conducted at minimum on an annual basis, and that it is the responsibility of the Privacy Officer to initiate privacy audits.

Inscyte's policies and procedures state that Privacy Impact Assessments are to be maintained in perpetuity in the Log of Privacy Impact Assessments in the privacy document archives. This includes privacy impact assessments that have been completed, those that are in progress but no yet completed, and those that have been requested but not yet undertaken. It is the responsibility of the Privacy Officer to ensure that the Log of Privacy Impact Assessments in maintained accurate and up to date.



Inscyte requires its agents to comply with its Policies and Procedures in respect of Privacy Impact Assessments. The Privacy Officer is responsible for monitoring and enforcing compliance. The policies and procedures further describe the consequences of breach and that compliance will be audited in accordance with the Inscyte's Policy and Procedures In Respect of Privacy Audits, to be held at minimum on an annual basis, and that the Privacy Officer is responsible for initiating privacy audits.

Inscyte's policies and procedures require all agents of Inscyte to be vigilant of and notify Inscyte's Privacy Officer, at the first reasonable opportunity, in accordance with Inscyte's Policy and Procedures for Privacy Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.

26. Log of Privacy Impact Assessments

Inscyte Corporation maintains a Log of Privacy Impact Assessments that includes assessments that have been commissioned but not yet started, assessments that are underway, and assessments that have been completed. The log of Privacy Impact Assessments contains the following information at minimum:

a) The date the Privacy Impact Assessment was commissioned
b) The subject (data holding or system) of the Privacy Impact Assessment
c) The status of the Privacy Impact Assessment (pending, underway, completed)
d) The name(s) of the individual(s) conducting the assessment
e) The expected/actual date of completion of the assessment
f) The recommendations of the assessment
g) The review status of the recommendations
h) A description of the manner in which each recommendation will be addressed
i) The target date for addressing each recommendation
j) The agent(s) responsible for addressing each recommendation

Inscyte's policies and procedures designate the Privacy Officer as being responsible for reviewing the recommendations arising from Privacy Impact Assessments, for establishing timelines to address the recommendations and for delegating work to other agents to implement the recommendations, and for monitoring and ensuring that the recommendations are implemented in a timely and effective manner.

In addition, Inscyte's policies stipulate that recommendations emanating from Privacy Impact Assessments to mitigate identified risks shall be recorded in the Corporate Risk Register, together with anticipated actions and dates that the actions will be completed.

Inscyte Corporation also maintains a Log of Data Holdings of personal health information and an Asset Inventory of information and security systems components. These documents indicate if

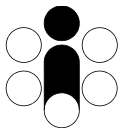
Privacy Impact Assessments were performed with respect to the data holdings or information and security systems components, and indicate if and when Privacy Impact Assessments were performed on these assets, and the reasons that Privacy Impact Assessments were not performed on these assets, together with the names and dates of the agents responsible for making this determination.

27. Policy and Procedures in Respect of Privacy Audits

Inscyte Corporation has developed and implemented policies and procedures in respect of conducting privacy audits to assess compliance with its privacy policies, procedures and practices by Inscyte and its agent(s) permitted to access and use personal health information pursuant to Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information.
Inscyte's policies and procedures state that the purpose of the privacy audit is to monitor the privacy program and document archives to ensure that day-to-day activities are in compliance with Inscyte's Privacy and Security Policies and Procedures and that all related documentation is up-to-date, complete and accurate. The policies further state that the privacy audit is an internal self-assessment tool to collect information to inform the planning and decision-making process regarding the on-going application of privacy legislation to Inscyte's organization. Inscyte Corporation does not conduct audits of its member medical laboratories, health information custodians, or prescribed persons/entities under the Act to whom it discloses, or from whom it collects, personal health information.

Inscyte conducts both privacy audits and security audits. There is only one type of privacy audit. The policies state that the privacy audit shall be conducted on an annual basis, usually in conjunction with the annual review of policies and procedures, typically scheduled in October of each year. The policies state that the annual privacy audit involves:

a) Reviewing changes to applicable legislation and applicable orders and/or best practice guidelines issued by the Office of the Privacy Commissioner, Ontario
b) Reviewing the status of personal health information holdings
c) Reviewing uses of personal health information
d) Reviewing the status of all security measures, including;
    a. Status of user accounts to information systems
    b. Status of personal access cards/keys to secure premises
e) Reviewing privacy documentation to ascertain completeness and accuracy, including;
    a. Data sharing agreements
    b. Third party service agreements
    c. Log of privacy training sessions and attendance
    d. Log of privacy breaches
    e. Log of privacy complaints
    f. Log of security audits
    g. Log of security breaches



h. Log of privacy audits
i. Log of privacy impact assessments
j. Log of transfers of personal health information
k. Log of data holdings
l. Log of individuals having access to personal health information
m. Corporate risk register
n. Consolidated log of recommendations

The results of the reviews and any recommendations are documented in the Log of Privacy Audits. The policies stipulate that it is the responsibility of the Privacy Officer to initiate a privacy audit and delegate specific reviews to designated members of Inscyte's or its agent's staff. Inscyte's Privacy Officer has been delegated day-to-day authority to manage the privacy program while the Security Officer has been delegated day-to-day authority to manage the security program.

The process of conducting a privacy audit involves reviewing and assessing the status of the items listed above in relation to the requirements articulated in Inscyte's Privacy & Security Policies and Procedures. The results of each review are required to be documented indicating:

a) The item under review (e.g. Log of Privacy Breaches)
b) The name of the reviewer
c) The date the review was started
d) Findings with respect to compliance with requirements
e) Identified issues (if any)
f) Recommended remedial actions (if any)
g) The date of completion

Following the review and documentation of each item, the Privacy Officer is responsible for consolidating the review documentation and convening a panel of representatives from Inscyte and its agent(s) to review and discuss the results and make consolidated recommendations to address any privacy or security issues arising. The policy requires that these recommendations are to be documented in the *Consolidated Log of Recommendations* together with actions, target dates and personnel responsible for addressing each recommendation. It is the responsibility of the Privacy Officer to ensure that items within the *Consolidated Log of Recommendations* are acted upon in the required time frames.

At the conclusion of the privacy audit, the policies require the review documentation and consolidated recommendations to be archived in Inscyte's privacy document archives and a copy forwarded to the President of Inscyte within thirty (30) days of completion. Further, the policies require that the privacy audit activity is recorded in the *Log of Privacy Audits*. It is the responsibility of the Privacy Officer to communicate the findings and recommendations of

privacy audits to appropriate parties and to ensure that the *Log of Privacy Audits* is complete and up-to-date.

Inscyte's policies and procedures require all agents of Inscyte to be vigilant of and notify Inscyte's Privacy Officer, at the first reasonable opportunity, in accordance with Inscyte's Policy and Procedures for Privacy Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.

28. Log of Privacy Audits

Inscyte Corporation maintains a *Log of Privacy Audits* that have been completed. The log contains the following information:

a) A unique privacy audit number
b) The date the privacy audit was started
c) The date the privacy audit was completed
d) The location of the review documentation
e) Summary of findings and recommendations

The personnel or agent(s) responsible for addressing each recommendation; the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed is recorded in Inscyte's *Consolidated Log of Recommendations* referencing the unique privacy audit number as the source of the recommendations.

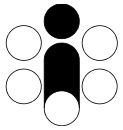
The policies and procedures state that it is the responsibility of the Privacy Officer to initiate a privacy audit, at minimum on an annual basis, for delegating work to appropriate agents in carrying out the audit, and for ensuring that the audit is completed.

29. Policy and Procedures for Privacy Breach Management

Inscyte Corporation has developed and implemented policies and procedures that address the identification, reporting, containment, notification, investigation, and remediation of privacy breaches.

The policy defines a "breach of privacy" as:

a) The collection, use, disclosure, retention, or disposal of personal health information that is in contravention of applicable laws, including, but not limited to Ontario's Personal Health Information Protection Act, 2004 and its regulations.
b) Failure to adhere to Inscyte's Privacy & Security Policies and Procedures



c) A breach of a contractual agreement for the handling of personal health information such as Confidentiality and Non-Disclosure Agreements with agents of Inscyte or its agent(s) or Data Sharing Agreements with third parties.
d) Circumstances where personal health information is stolen, lost or subject to unauthorized use or disclosure or where records of personal health information are subject to unauthorized copying, modification, or disposal.

The policy and procedures impose a mandatory requirement on Inscyte's agents to notify the Privacy Officer of Inscyte if a privacy breach or suspected privacy breach is discovered. The policies state that this notification is to be made immediately, either verbally or by email describing the incident, the time and place of discovery, the nature of the information involved, and containment actions taken (if any).

The policies state that upon discovery of a breach of privacy (or suspected breach of privacy) the following actions shall be taken:

1. Assess the incident
2. Contain the breach
3. Notify the Privacy Officer and Security Officer
4. Initiate a Privacy Breach Report
5. Notify appropriate parties
6. Investigate and remediate the breach
7. Complete the Privacy Breach Report and submit to Privacy Officer for sign-off
8. Approve and sign-off of the Privacy Breach Report
9. Approve and act on recommendations for mitigating strategies

Inscyte's policies state that depending on the nature and severity of the breach, these actions may have to be undertaken simultaneously, or in short succession.

Inscyte's policies and procedures stipulate that the first course of action upon discovery of a breach or possible breach of privacy is to assess the incident to determine whether a privacy breach has in fact occurred and if so, what, if any, personal health information has been breached. This determination can be made by any agent of Inscyte.

The policies and procedures stipulate that in the event that personal health information has been breached the immediate action to be taken is to contain the breach. The policies and procedures provide guidelines with respect to containment procedures, depending on the format and media of the personal health information that has been breached, to ensure that steps are taken to protect the personal health information from further theft, loss or unauthorized use or disclosure, copying, modification or disposal. The procedures require, where possible, that the records of personal health information be retrieved and returned to Inscyte to be retained in

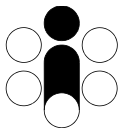
secure storage or disposed of in a secure manner. In case of disposal, written confirmation must be provided to Inscyte of the date and time of disposal, the method, who disposed of the information, and where the disposal took place.

The containment procedures further require that steps be taken to ensure that additional privacy breaches cannot occur through the same mechanism by assessing whether the breach would allow unauthorized access to any other information and taking necessary actions to prevent recurrence, such as shutting down computer servers, networks etc.

It is the responsibility of the Privacy Officer to review the containment measures and assess if the breach has been fully contained and that all personal health information that can be retrieved has been retrieved and returned to secure storage or securely disposed of. It is the responsibility of the Security Officer to ensure that security measures that may have been compromised are either disabled or reset to prevent recurrence of the breach.

Inscyte's policies and procedure require a *Privacy Breach Report* to be initiated and completed for all incidence of breach or suspected breach, regardless of the severity or consequences of the breach. The policies set out the minimum content of a *Privacy Breach Report* as follows:

(a) Unique report number
(b) The date the breach was reported to Inscyte
(c) The name of the person(s) reporting the breach
(d) The name of the author(s) of the report (investigators)
(e) The date/time of the breach incident (or estimate thereof)
(f) The evidence of breach (what lead to the discovery of breach)
(g) The nature/source of the personal health information involved
(h) The amount of personal health information involved (or estimate thereof)
(i) The format of the personal health information (paper, media, etc.)
(j) The location of the personal health information
(k) The nature of the breach (or potential breach) categorized as one or more of:
    a. Inappropriate collection/receipt of personal health information
    b. Inappropriate use of personal health information
    c. Inappropriate disclosure of personal health information
    d. Inappropriate retention of personal health information
    e. Inappropriate disposal of personal health information
    f. Failure to follow prescribed policies and/or procedures
    g. Failure to adhere to contractual terms and conditions
(l) Who perpetrated the breach (internal/external)
(m) The motivation/cause for the breach (e.g. accidental, purposeful)
(n) The mechanism of the breach (i.e. method, process failure, etc.)
(o) Containment procedures taken and dates (what was done to contain the breach)



(p) Likelihood of disclosure of personal health information to unauthorized parties
(q) List of parties and personnel contacted/notified
(r) Indication if affected persons were contacted (names & dates)
(s) Indication if IPC was contacted (date)
(t) Remedial actions taken and recommendations for mitigating strategies
(u) Privacy Officer sign-off and date

It is the responsibility of the Privacy Officer to ensure that a *Privacy Breach Report* is initiated in all cases within five (5) business days of receiving notification, and to delegate investigation activities to appropriate personnel. It is the responsibility of the Privacy Officer to ensure that all breaches are investigated and that reports are completed in a reasonable time frame. It is the responsibility of the Privacy Officer to sign-off and approve of Privacy Breach Reports and resulting recommendations for mitigating strategies to prevent similar breaches from occurring in the future. The policies further state that the Privacy Breach Report provides the contact information of the Privacy Officer.

In the event that there is reasonable cause to believe that personal health information has been disclosed to unauthorized parties, or is likely to be disclosed as a consequence of the breach, Inscyte's breach management policy requires the Privacy Officer to immediately notify the President of Inscyte about the breach, either verbally or by email and to provide a copy of the interim *Privacy Breach Report*. The policy states that is subsequently the responsibility of the President of Inscyte to notify, at the first reasonable opportunity, the health information custodians or parties to data sharing agreements affected/impacted by the breach, and to notify the Office of the Information and Privacy Commissioner of Ontario. This notification can be made verbally, by email or in writing, with a copy of the interim Privacy Breach Report.

The Privacy Officer of Inscyte has been delegated day-to-day authority to manage the privacy program. As such, it is the responsibility of the Privacy Officer to assign appropriate personnel to investigate and document each incident of breach. The investigation process requires addressing each section of the *Privacy Breach Report* using any appropriate means such as document reviews, interviews, site visits, inspections etc. This includes making recommendations for mitigating strategies to prevent similar breaches from occurring in the future. The investigators are responsible for preparing the *Privacy Breach Report* and submitting it to the Privacy Officer for review and final approval.

Upon approval recommendations made in a *Privacy Breach Report* are recorded in Inscyte's *Consolidated Log of Recommendations*, citing the report number as the source of the recommendations and specifying the actions to be taken to implement the recommendations, the personnel responsible for carrying out the actions, and the target date(s) of completion.

Inscyte's policies and procedures distinguish between a breach of privacy and a breach of security. Inscyte's policies define a "breach of security" as:

a) An unauthorized person gaining access to, or attempting to gain access to, secured premises or secured information, by any means whatsoever.
b) An act that compromises the confidentiality, integrity (accuracy and completeness) or availability of secured information.

Inscyte's policy states that although a breach of security can occur without a consequential breach of privacy (and vice-versa) the process to be followed in identifying, reporting, containing, notifying, investigating and remediating a security breach is the same as that for a privacy breach, and if in the course of the investigation of a security breach it is discovered that a privacy breach may also have occurred, then the policies and procedures in respect of managing a privacy breach also apply.

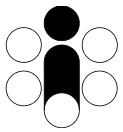
Inscyte's policy and procedure require that a perpetual *Log of Privacy Breaches* be maintained in its privacy document archives containing a summary listing of privacy breaches and the complete *Privacy Breach Report* on each incident. The policy designates the Privacy Officer as being responsible for ensuring that the log is accurate and up-to-date, and for tracking that the recommendations arising from the investigation of privacy breaches are addressed within the identified timelines.

Inscyte's policies and procedures require all agents of Inscyte to be vigilant of and notify Inscyte's Privacy Officer, at the first reasonable opportunity, in accordance with Inscyte's Policy and Procedures for Privacy Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures. The policies and procedures also set out the consequences of breach. Inscyte's policy stipulates that compliance will be audited in accordance with its Policy and Procedures In Respect of Privacy Audits, which set out the frequency with which the policy and procedures are audited and designate the Privacy Officer as being responsible for conducting the audit and for ensuring compliance with Inscyte's policy and its procedures.

In developing its policies and procedures, Inscyte has given regard to the guidelines produced by the Information and Privacy Commissioner of Ontario entitled "What to do When Faced With a Privacy Breach: Guidelines for the Health Sector."

30. Log of Privacy Breaches

Inscyte Corporation maintains a perpetual *Log of Privacy Breaches* in its privacy document archives containing a summary listing of privacy breaches and the complete *Privacy Breach Report* on each incident. The information in the log includes:



a) The date the privacy breach was reported.
b) The date that the privacy breach was identified or suspected.
c) Whether the privacy breach was internal or external.
d) The nature of the personal health information that was the subject matter of the privacy breach and the nature and extent of the privacy breach.
e) The date that the privacy breach was contained and the nature of the containment measures.
f) The date that the health information custodian or other organization that disclosed the personal health information to the prescribed person or prescribed entity was notified.
g) The date that the investigation of the privacy breach was completed.
h) The agent(s) responsible for conducting the investigation.
i) The recommendations arising from the investigation.

The following information is retained in Inscyte's *Consolidated Log of Recommendations* for each incident of breach:

a) The recommendation description together with the reference to the Privacy Breach Report number from which the recommendations emanated.
b) The personnel responsible for addressing each recommendation.
c) The date each recommendation was or is expected to be addressed; and
d) The manner in which each recommendation was or is expected to be addressed.

31. Policy and Procedures for Privacy Complaints

Inscyte Corporation has developed and implemented policies and procedures to address the process to be followed in receiving, documenting, tracking, investigating, remediating, and responding to privacy complaints. The policies define a "privacy complaint" as being a concern or complaint relating to the privacy policies, procedures and practices implemented by Inscyte Corporation and related to Inscyte Corporation's compliance with the Act and its regulation.

The policy states that Inscyte shall make its complaint process and standard *Privacy Compliance Challenge Form* freely available to the public on its website together with the contact information of the President of Inscyte and the Privacy Officer of Inscyte, designated as the individuals to whom all complaints should be addressed. The policies further state that all filed complaints shall be brought to the attention of the President. In addition, Inscyte's policy states that individuals shall also be advised that they may make a complaint regarding Inscyte's compliance with the Act and its regulation to the Information and Privacy Commissioner of Ontario and that the mailing address and contact information for the Information and Privacy Commissioner of Ontario shall be provided on Inscyte's public website.

The policy and procedures establish the process to be followed in receiving privacy complaints. All complaints must be documented using Inscyte's standard *Privacy Compliance Challenge Form*

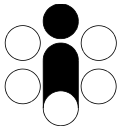
and include supporting information and/or other documentation relevant to the complaint. The procedures require that a complainant provide this information to the President or Privacy Officer of Inscyte in paper or electronic format.

The policy states that Inscyte Corporation will investigate all complaints. It is the responsibility of the President of Inscyte to delegate duties to appropriate agents of Inscyte to investigate a complaint (e.g. carry out document reviews, interviews, site visits, inspections) and to make recommendations regarding actions to be taken to resolve the complaint. The policies require that all investigations are to be documented using Inscyte's standard *Complaint Investigation and Resolution Form*. It is also the responsibility of the President of Inscyte, at the first reasonable opportunity, to notify any related parties to the complaint, which may include related health information custodians, ministries of government and the Office of the Information and Privacy Commissioner of Ontario.

The policies state that all complaints shall be investigated in a timely manner, which may involve seeking additional information from the complainant and consultation with affected parties. The policies require that the complainant be notified, in writing, of the investigation undertaken, what the investigation will consist of, whether the complainant will be contacted for further information about the complaint, the time frame expected for resolution, and the contact information of the person(s) to whom the complainant may make inquiries regarding the progress and status of the investigation and the documentation that will be provided to the individual following the investigation. The policy identifies the agent responsible for sending out the above-noted letter and the timeframe within which the letter will be sent to the individual. Further, the policies state that the individual making the privacy complaint shall also be advised that he or she may make a complaint to the Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that the Act or its regulation has been or is about to be contravened and the contact information for the Information and Privacy Commissioner of Ontario shall also be provided.

In the event that an investigation into a privacy complaint reveals that a breach of privacy or potential breach of privacy has occurred then the provisions of Inscyte's policies and procedures regarding breach management shall take effect and the breach shall be contained, managed and remediated in accordance with those policies and procedures in addition to the process of resolving the privacy complaint.

Inscyte's policies state that at the conclusion of a complaint investigation a written report shall be prepared describing the results of the investigation together with recommendations regarding actions to be taken to resolve the complaint. This report shall be provided to the complainant and all related parties, including, if applicable, the Office of the Information and Privacy Commissioner of Ontario. It is the responsibility of the President of Inscyte to ensure that the report is delivered to the appropriate parties in a timely manner.



The policies state that upon conclusion of the investigation, if a complaint is deemed justified, Inscyte Corporation will take appropriate and reasonable measures to remedy and resolve the complaint including, if necessary, amending its *Privacy & Security Policies and Procedures*. It is the responsibility of the President of Inscyte to make this determination. The policies require that the measures taken with respect to the resolution of a complaint shall be communicated to the complainant, affected parties and, if applicable, to the Office of the Information and Privacy Commissioner of Ontario, in a *Letter of Complaint Resolution*, containing the measures taken and the dates of implementation. It is the responsibility of the President of Inscyte to ensure that the *Letter of Complaint Resolution* is delivered to the complainant and appropriate parties in a timely manner.

Inscyte's Privacy & Security Policies and Procedures stipulate that Inscyte's Privacy Officer has been delegated day-to-day authority to manage the privacy program while the Security Officer has been delegated day-to-day authority to manage the security program. It is the responsibility of the Privacy Officer to ensure that recommendations for changes to the privacy and security practices emanating from complaint investigations are acted upon and recorded in Inscyte's *Consolidated Log of Recommendations* including:

a) The recommendation description together with the reference to the Complaint number from which the recommendation emanated.
b) The personnel responsible for addressing each recommendation.
c) The date each recommendation was or is expected to be addressed; and
d) The manner in which each recommendation was or is expected to be addressed.

Inscyte's policy and procedures require that a perpetual *Log of Privacy Complaints* be maintained in Inscyte's privacy document archives and identifies the Privacy Officer as being responsible for maintaining the log and for tracking whether the recommendations arising from the investigation of privacy complaints are addressed within the identified timelines. The Log of Privacy Complaints identifies each complaint using a unique number and includes complete copies of documentation related to each complaint, including the *Privacy Compliance Challenge Form,* the *Complaint Investigation and Resolution Form,* and the *Letter of Complaint Resolution.*

Inscyte requires its agents to comply with its policies and procedures regarding privacy complaints and designates the Privacy Officer as being responsible for monitoring and ensuring compliance. The policy and procedures also set out the consequences of breach. Inscyte's policy and procedures in respect of privacy and security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Privacy Officer to initiate privacy audits and the responsibility of the Security Officer to initiate security audits at the prescribed intervals. The procedures

outline the steps involved and the data and documentation holdings that are to be audited and how the results of the audits are to be documented.

Inscyte's policy and procedures with respect to privacy complaints further stipulate that in the event that a complaint reveals a breach or potential breach of privacy, then Inscyte's policies and procedures regarding privacy breach management shall also take effect.

32. Log of Privacy Complaints

Inscyte Corporation maintains a *Log of Privacy Complaints* that includes a summary of all received complaints including:

- The date that the privacy complaint was received.
- A unique complaint number.
- The nature of the complaint
- The date that the individual making the complaint was advised that the complaint will be investigated.
- The personnel assigned to conducting the investigation.
- The dates that the investigation was commenced and completed.
- The recommendations arising from the investigation
- The date that the individual making the privacy complaint was advised of the findings of the investigation and the measures taken, if any, in response to the privacy complaint; or the date that the individual was advised that the complaint will not be investigated.

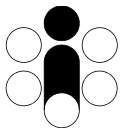
In addition, the privacy document archives contain the complete documentation related to each complaint, consisting of the *Privacy Compliance Challenge Form,* the *Complaint Investigation and Resolution Form,* and the *Letter of Complaint Resolution*.

The following information is also retained in Inscyte's *Consolidated Log of Recommendations* for each complaint:

a) The recommendation description together with the reference to the Complaint number from which the recommendation emanated.
b) The personnel responsible for addressing each recommendation.
c) The date each recommendation was or is expected to be addressed; and
d) The manner in which each recommendation was or is expected to be addressed.

33. Policy and Procedures for Privacy Inquiries

Inscyte Corporation has developed and implemented policies and procedures to address the process to be followed in receiving, documenting, tracking, and responding to privacy inquiries. The policies define a "privacy inquiry" as a question regarding Inscyte's privacy and security



policies, procedures and practices and related to Inscyte Corporation's compliance with the Act and its regulation.

The policy states that Inscyte shall make its inquiry process and standard *Privacy Inquiry Form* freely available to the public on its website together with the contact information of the President of Inscyte and the Privacy Officer of Inscyte, designated as the individuals to whom all inquiries should be addressed. The policies also stipulate that Inscyte's Privacy Code, and its Privacy & Security Policies and Procedures shall be available to the public on its website together with frequently asked questions and answers.

The procedure for handling privacy inquiries state that Inscyte's standard *Privacy Inquiry Form* will be provided to the inquirer for submitting an inquiry and that the inquiry will be logged in Inscyte's *Log of Privacy Inquiries*, which includes at minimum, the following information:

a) A unique inquiry identification number
b) The date of the inquiry
c) The name(s) of the person(s) making the inquiry
d) A summary of the nature of the inquiry
e) The status of the inquiry (posted, in progress, completed)
f) The date of response
g) The name of the person making the response
h) A summary of the response
i) A copy of the Privacy Inquiry Form
j) A copy of the Response Letter

The policies state that it is the responsibility of the Privacy Officer to ensure that all inquiries are logged, documented and responded to in a timely manner and to delegate tasks to appropriate personnel in order to prepare a *Letter of Response*, including informing the inquirer about the anticipated date of response. The policies set out the format and minimum content of the *Letter of Response*. Further, the policies require the Privacy Officer to review and approve all *Letters of Response* prior to delivering the response to the inquirer.

In the event that activities related to a privacy inquiry lead to a complaint being filed then the provisions of Inscyte's policies and procedures regarding privacy complaints shall take effect.

In the event that activities related to a privacy inquiry reveal that a breach of privacy or potential breach of privacy has occurred then the provisions of Inscyte's policies and procedures regarding breach management shall take effect and the breach shall be contained, managed and remediated in accordance with those policies and procedures.

Inscyte requires its agents to comply with its policies and procedures regarding privacy inquiries and designates the Privacy Officer as being responsible for monitoring and ensuring compliance. The policies and procedures set out the consequences of breach. Inscyte's policy and procedures in respect of privacy and security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Privacy Officer to initiate privacy audits and the responsibility of the Security Officer to initiate security audits at the prescribed intervals. The procedures outline the steps involved and the data and documentation holdings that are to be audited and how the results of the audits are to be documented.

Part 2 – Security Documentation

1. Information Security Policy

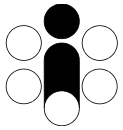
Inscyte Corporation has a comprehensive and overarching information security policy in place to protect personal health information received by Inscyte under the Act. The information security policy requires that reasonable and effective steps are taken to ensure that the personal health information in the custody of Inscyte is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information are protected against unauthorized copying, modification or disposal.

The information security policy states that Inscyte Corporation is required to undertake comprehensive and organization-wide threat and risk assessments of all information security assets, including personal health information, as well as appropriate project specific threat and risk assessments. The policies prescribe a methodology for identifying, assessing, documenting, and remediating threats and risks and for prioritizing all threats and risks identified for remedial action.

The information security policy establishes a comprehensive information security program that implements administrative, technical, and physical security controls that meet with established industry standards and practices. The information security program addresses the threats and risks identified, is open to independent verification, and is consistent with Inscyte's and its agent's security framework and control objectives. The security policies and procedures specify that responsibility for the development and implementation of the security program rests with the Security Officer of Inscyte, who is also the Security Officer of Inscyte's agent Inspirata.

Inscyte's security policy requires the information security program to consist of the following control objectives and security policies, procedures, and practices:

- A security governance framework for the implementation of the information security program, including security training and awareness.



- Policies and procedures for the ongoing review of the security policies, procedures and practices implemented.

- Policies and procedures for ensuring the physical security of the premises.

- Policies and procedures for the secure retention, transfer and disposal of records of personal health information, including policies and procedures related to mobile devices, remote access and security of data at rest.

- Policies and procedures to establish access control and authorization including business requirements, user access management, user responsibilities, network access control, operating system access control and application and information access control.

- Policies and procedures for information systems acquisition, development and maintenance including the security requirements of information systems, correct processing in applications, cryptographic controls, security of system files, security in development and support procedures and technical vulnerability management.

- Policies and procedures for monitoring, including policies and procedures for maintaining and reviewing system control and audit logs and security audits.

- Policies and procedures for network security management, including patch management and change management.

- Policies and procedures related to the acceptable use of information technology.

- Policies and procedures for back-up and recovery.

- Policies and procedures for information security breach management; and

- Policies and procedures to establish protection against malicious and mobile code.

Inscyte's information security policy are organized around the above objectives and are broken down into detailed policies and procedures to address the above-noted matters.

The information security policy requires that Inscyte maintain comprehensive documentation describing its computing infrastructure and security controls including the transmission of personal health information over authenticated, encrypted and secure connections; the establishment of secured servers, firewalls, demilitarized zones and other perimeter defenses;

anti-virus, anti-spam and anti-spyware measures; intrusion detection and prevention systems; privacy and security enhancing technologies; and mandatory system-wide password-protected screen savers after a defined period of inactivity.

Inscyte's security policy also sets out the procedures for day-to-day monitoring of security controls to verify the effectiveness of the security program and to detect and deal with threats and risks to holdings of personal health information.

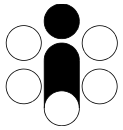
Inscyte requires its agents to comply with its security policies and procedures and designates the Security Officer as being responsible for monitoring and ensuring compliance. The policies and procedures set out the consequences of breach. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Security Officer to initiate security audits at the prescribed intervals. The procedures outline the steps involved and the data and documentation holdings that are to be audited and how the results of the audits are to be documented.

Inscyte's policy further requires its agents to notify Inscyte at the first reasonable opportunity, in accordance with the Policies and Procedures for Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or any of the security policies, procedures and practices.

2. Policy and Procedures for Ongoing Review of Security Policies, Procedures and Practices

Inscyte's Privacy & Security Policies and Procedures Manual includes policies and procedures governing the regular review of its security policies, procedures, and practices. The policies state that Inscyte shall review its security policies and procedures at minimum on an annual basis, or more frequently should there be changes in technology, best practices, or the Act and its regulation. The policies further state that a review of relevant policies and procedures shall be taken following a breach of privacy or security to determine if modifications to the policies and procedures are necessary to avert a similar breach in the future.

The policies state that it is the responsibility of the Privacy Officer to initiate a review process, that a committee shall be organized to carry out the review consisting of the Privacy Officer, the Security Officer and selected representatives from Inscyte's staff and associated health information custodians (e.g. member laboratories or prescribed persons/entities with whom Inscyte exchanges information). The policy and procedures identify the Security Officer as being responsible for amending and/or drafting new security policies, procedures and practices if deemed necessary as a result of the review. The policies state that in the event that proposed changes represent a material change to daily operations, the results and recommendations of



the review will be reported to the President of Inscyte and CEO of Inspirata for review and approval before the changes are implemented.

The policies state that the review process shall take into account any orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation; evolving industry security standards and best practices; technological advancements; amendments to the Act and its regulation relevant to the prescribed person or prescribed entity; and recommendations arising from privacy and security audits, privacy impact assessments and investigations into privacy complaints, privacy breaches and information security breaches. The review process also takes into account whether the security policies, procedures and practices of Inscyte Corporation continue to be consistent with its actual practices and whether there is consistency between and among the security and privacy policies, procedures and practices implemented.

The policies describe the procedure for amending and documenting policies and procedures and for communicating the amendments to agents and the public. Amended policies and procedures result in a revision of Inscyte's Privacy & Security Policies and Procedures Manual, which is made available through Inspirata's internal business network and to the public on Inscyte's website. The Privacy Officer is responsible for ensuring that emended policies and procedures are published and communicated to all affected parties and stakeholders.

Inscyte requires its agents to comply with its security policies and procedures and designates the Privacy Officer and the Security Officer as being responsible for monitoring and ensuring compliance. The policy also sets out the consequences of breach. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Security Officer to initiate security audits at the prescribed intervals. The procedures outline the steps involved and the data and documentation holdings that are to be audited and how the results of the audits are to be documented.

3. Policy and Procedures for Ensuring Physical Security of Personal Health Information

Inscyte Corporation has policies and procedures in place addressing the physical safeguards that are required to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal. Inscyte's agent Inspirata is responsible for implementing all necessary physical security safeguards at its premises to control access to locations where records of personal health information are retained, including zone-dependent individual-specific key card entry points, locked physical storage cabinets, intrusion detection and alarm systems.

Inspirata's premises are divided into zones and varying levels of security with each successive level being more secure and restricted to fewer individuals. Furthermore, to access locations where records of personal health information are retained or can be accessed via computer terminals requires individuals to pass through at least two audited security checkpoints.

Inscyte requires its agents to comply with its security policies and procedures and designates the Security Officer as being responsible for monitoring and ensuring compliance. The policy also sets out the consequences of breach. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Security Officer to initiate security audits at the prescribed intervals. The procedures outline the steps involved and the data and documentation holdings that are to be audited and how the results of the audits are to be documented.

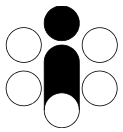
Inscyte's policy requires its agents to notify Inscyte at the first reasonable opportunity, in accordance with Inscyte's Policies and Procedures for Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or any of Inscyte's security policies, procedures and practices.

Policy, Procedures and Practices with Respect to Access by Agents

Inscyte Corporation's policies require that documentation be kept describing Inspirata's premises and the security control zones and access levels for various staff granted access to the premises. The security zones within Inspirata's premises are categorized as:

1) "General Offices" – require keycard access but does not contain PHI
2) "Secured Offices" – require at least two security checkpoints and may contain PHI
3) "Datacenter" – requires at least two security checkpoints and contains PHI

The policy and procedures identify the Security Officer as being responsible for receiving, reviewing, granting and terminating access by an agent of Inscyte to the premises and to locations within the premises where records of personal health information are retained, including the levels of access that may be granted. The policy and procedures further indicate to whom this determination will be communicated. The process of granting physical access to premises requires an individual to submit a standard access request form to the Security Officer setting out the individuals name, the date of the request, the individual's job functions, the zones to which the individual requests access, the time of day during which access is requested, and the duration for which access is requested. The Security Officer is responsible for reviewing and approving or denying the requests for access. In making this determination, the Security Officer must take into account reasonable access requirements in order for the individual to fulfill his/her job functions, employment, contractual or other responsibilities.



In the event that an individual requests access to a security zone where personal health information is retained or can be accessed, the policy requires the request to be further reviewed and approved/denied by the Privacy Officer. In making the determination to grant access to security zones containing personal health information, the Privacy Officer takes into consideration the "need to know" principle to ensure that access is only provided to a limited number of persons who routinely require access to personal health information for their job functions, employment, contractual or other responsibilities.

Specifically, Inscyte's security policies state that as best practice, keys, pass cards, or access codes to physical security checkpoints should only be issued to employees of Inscyte or Inspirata. and not to contracted individuals or third parties. Furthermore, the policies set out minimum criteria for granting access to different categories of security zones as follows.

An employee shall be issued keys, pass cards, or access codes to general offices provided that:

a) The employee has completed his/her probationary period of employment.
b) The employee has executed a signed and witnessed Personal Health Information Confidentiality and Non-Disclosure Agreement.
c) The employee requires access to general offices.
d) Approval has been given by the Security Officer.

An employee shall be issued keys, pass cards, or access codes to secured offices where personal health information is stored and used provided that:

a) The employee has completed his/her probationary period of employment.
b) The employee is required to work with personal health information.
c) The employee has executed a signed and witnessed Personal Health Information Confidentiality and Non-Disclosure Agreement.
d) The employee has received privacy & security awareness training.
e) Approval has been given by the Privacy Officer.

An employee shall be issued keys, pass cards, or access codes to the datacenter where personal health information is stored provided that:

a) The employee has completed his/her probationary period of employment.
b) The employee is required to work in the datacenter.
c) The employee has executed a signed and witnessed Personal Health Information Confidentiality and Non-Disclosure Agreement.
d) The employee has received privacy & security awareness training.
e) Approval has been given by the Privacy Officer.

Where physical access rights are granted to an individual for a limited period of time, it is the responsibility of the Security Officer to monitor and ensure that the access rights are terminated at the expiry of the stated time period.

In practice, employees of Inscyte or its agent Inspirata are only issued electronic access cards and not physical keys. The issuing, activation, and de-activation of electronic access cards is a strictly controlled process that can only be performed by individuals authorized to do so by the Security Officer. Access cards are stored in a combination-lock safe and the software for activating, de-activating and monitoring access card usage is account/password protected and available in the secure datacenter only. Access rights to administer the electronic access card system are limited to three individuals. Each access card is linked to a specific employee and the system records the use of the cards at each security checkpoint noting the date/time of use, the checkpoint name, the success/failure of the card and the corresponding name of the employee to whom the card was issued.

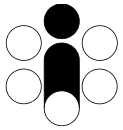
The electronic access card system is a software-controlled security network. Inscyte's security policies state that when a card is created, the operator must specify the following properties for each card:

a) The name of the employee to whom the card is issued
b) The security checkpoint(s) that the card will open
c) The times-of-day during which the card will open the specified checkpoints
d) The timeout (idle) period after which the card will automatically expire
e) Whether the card will be perpetual or expire upon a specified date

The policies and procedures further state that upon receipt of an access card the employee must sign a *Keycard Sign-out and Declaration* form that sets out the terms and conditions under which the card is issued to the employee and the responsibilities of the employee in that regard. The policies require that signed copies of all *Keycard Sign-out and Declaration* forms be retained in perpetuity in the privacy document archives.

Inscyte's security policies require maintaining a *Log of Individuals Having Access to Premises* to document the activation and de-activation of access cards to individuals and designate the Security Officer as being responsible for maintaining the log up-to-date and accurate. The policies require that the *Log of Individuals Having Access to Premises* be updated every time a change in access rights for an individual occurs. The log contains the following information:

a) The log entry date
b) The name/title of the individual to whom the entry pertains
c) The access card identification number
d) The security zone(s) to which access has been granted or terminated
e) The time-of-day restrictions on the access rights to each security zone
f) The expiry date of access to each security zone (if applicable)
g) The name/title of the person that granted or terminated access



h) The name/title of the person approving the granting of access rights
i) The date access rights were granted or terminated
j) Description of the reasons for granting or terminating access rights

Theft, Loss and Misplacement of Identification Cards, Access Cards and Keys

Inscyte's policy and procedures require agents of Inscyte to notify the Security Officer at the first reasonable opportunity of the theft, loss or misplacement of identification cards, access cards and/or keys. This notification can be made verbally or by email and must indicate the time and circumstances under which the theft, loss or misplacement occurred. Upon receiving notification, it is the responsibility of the Security Officer to ensure that appropriate measures are taken to disable the access rights of the access cards or keys in question. It is also the responsibility of the Security Officer to log the event in the *Log of Individuals Having Access to Premises* and to re-issue new identification cards, access cards or keys as appropriate. In practice, only electronic access cards are issued to agents and not physical keys. One feature of the electronic access card system is that if a card is not used during a specified period of time (e.g. 3 days) the card will automatically expire and become useless.

Since the security system automatically expires (de-activates) cards depending on the properties specified at the time an access card is issued, there is no need for policies and procedures to issue and recover temporary or replacement cards. In the event of theft, loss or misplacement of a card, the policies and procedures state that the lost or stolen card be de-activated (if it has not automatically expired) and that a new card be produced in accordance with the policy and procedure regarding issuing of access cards.

Termination of the Employment, Contractual or Other Relationship

Inscyte's policies and procedures require all agents of Inscyte and an agent's supervisor to notify the Security Officer of the termination of their employment, contractual or other relationship with Inscyte or Inspirata, and to return their identification cards, access cards and/or keys to the Security Officer on or before the date of termination of their employment, contractual or other relationship in accordance with the Policy and Procedures for Recovery of Keys, Pass Cards and Access Codes at Termination of Employment and Inscyte's Policy and Procedure for Actions at Termination of Employment or Contract.

Inscyte Corporation's policies also require that access to the premises be terminated and that it is the responsibility of the Security Officer to ensure that access cards are de-activated upon the cessation of the employment, contractual or other relationship in accordance with its Policy and Procedures for Recovery of Keys, Pass Cards and Access Codes at Termination of Employment and its Policy and Procedure for Actions at Termination of Employment or Contract.

Notification When Access is No Longer Required

The policy and procedures require that agents of Inscyte granted approval to access location(s) where records of personal health information are retained, as well as the agent's supervisor, to notify Inscyte when the agent no longer requires such access.

The policies state that notification may be made verbally or in writing to the Security Officer, as soon as is reasonably practical. It is the responsibility of the Security Officer to ensure that appropriate measures are taken to disable the access rights of the access cards or keys in question within three (3) business days of receiving the notification. It is also the responsibility of the Security Officer to log the event in the *Log of Individuals Having Access to Premises* indicating the date that access rights were terminated and the name of the individual who terminated the access rights.

Audits of Agents with Access to the Premises

Inscyte's policies and procedures with respect to conducting security audits require a review of all persons with access rights to premises where records of personal health information are stored to ensure that these individuals continue to require the same level of access in accordance with their job functions or contractual obligations. The policies state that Security Audits shall be conducted on an annual basis in conjunction with Inscyte's annual privacy and security policy review process.

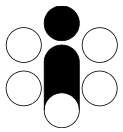
The Security Officer is responsible for conducting security audits. In the event that a security audit reveals that an individual no longer requires access to premises where records of personal health information are stored, the policies require the Security Officer to ensure that appropriate measures are taken to disable the access rights of the access cards or keys in question within three (3) business days and to log the event in the *Log of Individuals Having Access to Premises* indicating the date that access rights were terminated and the name of the individual who terminated the access rights.

Tracking and Retention of Documentation Related to Access to the Premises

Inscyte's policies and procedures requires that employees sign a *Keycard Sign-out and Declaration* form upon receipt of access rights that sets out the terms and conditions under which the card is issued to the employee and the responsibilities of the employee in that regard. The policies require that signed copies of all *Keycard Sign-out and Declaration* forms be retained in perpetuity in the privacy document archives and that it is the responsibility of the Security Officer to maintain this documentation. See also section 4, "Log of Agents with Access to the Premises of the Prescribed Person or Prescribed Entity", below for details.

Policy, Procedures and Practices with Respect to Access by Visitors

Inscyte's policies and procedures require that all visitors who may be required to enter secured premises where personal health information is stored, or could be accessed, must be registered



in a *Visitor Log* prior to being admitted to the secured premises and must be escorted and supervised during the visit by an agent who has access rights to the secured premises. Under these circumstances each visitor is required to provide:

a) His/her name
b) Name of associated business or organization
c) Reason for visit
d) Name of the person with whom the visitor is meeting
e) Name of the agent supervising the visit
f) Arrival date & time + signature of visitor
g) Departure time + signature of visitor

The policies and procedures require this information to be recorded in a perpetual *Visitor Log*, either in hardcopy or electronic format. All items are mandatory. It is the responsibility of the Security Officer to ensure that *Visitor Logs* are transferred to electronic format and retained in the privacy document archives.

The policies and procedures also require that visitors be accompanied by an agent at all times and as such do not require visitors to wear identification tags. The policies and procedures require the supervising individual to ensure that visitors sign the *Visitors Log* upon arrival and departure. In the event that a visitor departs without signing the log, the supervising individual is required to sign-out on behalf of the visitor.

4. Log of Agents with Access to the Premises of the Prescribed Person or Prescribed Entity

Inscyte's security policies require maintaining a *Log of Individuals Having Access to Premises* to document the activation and de-activation of access cards to individuals and designate the Security Officer as being responsible for maintaining the log up-to-date and accurate. The policies require that the *Log of Individuals Having Access to Premises* be updated every time a change in access rights for an individual occurs. The policies require the log to contain the following information at minimum:

a) The log entry date
b) The name/title of the individual to whom the entry pertains
c) The associated access card identification number
d) The security zone(s) to which access applies (which restricts access to PHI)
e) The time-of-day restrictions on the access rights to each security zone
f) The expiry date of access to each security zone (if applicable)
g) The name/title of the person that granted, changed, or terminated access
h) The name/title of the person approving the action

i) The date the access rights (cards) were granted, changed, or terminated (returned)
j) The date of the next audit of access
k) Description of the reason for granting, changing, or terminating access rights

The policies also require the *Log of Individuals Having Access to Premises* to be maintained in perpetuity in Inscyte's privacy document archives.

5. Policy and Procedures for Secure Retention of Records of Personal Health Information

Inscyte Corporation has developed and implemented policies and procedures with respect to the secure retention of records of personal health information in paper and electronic format.

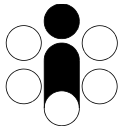
The policies and procedures address the retention periods for each holding of personal health information in various formats and media and stipulate that records shall not be retained for longer than the specified retention period. Inscyte's data sharing agreements with health information custodians also specify the retention period for the information in question.

With respect to the CytoBase database, the retention period is indefinite (i.e. perpetual) since CytoBase serves as a longitudinal electronic medical record of historical cervical cancer screening test results. The information is retained in identified form since all historical results on a woman are matched to new test orders at participating laboratories using the patient's Ontario health insurance number, surname and date of birth. Clinicians also use these identifiers to look up their patients' records using the CytoBase for Clinicians online service.

Inscyte does not use personal health information for research purposes and does not enter into research agreements with third parties. As such, there are no policies governing the retention of personal health information related to research projects.

The security policies and procedures require records of personal health information to be retained in a secure manner and designate the Security Officer as being responsible for ensuring the secure retention of these records. The policies and procedures specify the minimum technical security controls that must be applied to personal health information in paper and electronic formats to protect against theft, loss and unauthorized use or disclosure and to ensure that records of personal health information are protected against unauthorized copying, modification or disposal.

The policies set out the specific methods by which records of personal health information in paper and electronic format are to be secured. The policies require paper-based records to be stored behind at least two physical security checkpoints. The policies require that records stored



on portable storage media (e.g. CDs or USB keys) to be password protected and encrypted, and physically stored behind at least two physical security checkpoints. In the case of CD/DVD and USB keys for example, files containing PHI can be first encrypted and then packaged in a password protected ZIP archive file. In this case, both a password and a decryption key would be required to access the information. In the case of backup tapes, the information is hardware compressed and can only be retrieved using a specific tape drive. The policies also specify the minimum encryption key strength and set out minimum password length and composition rules to ensure strong passwords are used.

Inscyte's security policies and procedures also require all agents of Inscyte to take steps that are reasonable in the circumstances to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure and to ensure that records of personal health information are protected against unauthorized copying, modification or disposal. The policies require all personnel to be aware of what constitutes personal health information and to be vigilant of the potential for improper storage, use, disclosure, copying, modification, or disposal of such information, to confine records of personal health information to secure storage in the event that improper storage conditions are discovered, and to report potential breaches of security policies at the first available opportunity to the Security Officer and/or the Privacy Officer in accordance with Inscyte Corporation's policies and procedures with respect to security breach management.

Inscyte Corporation has contracted Inspirata to manage the secure collection, retention, transfer, and disposal of personal health information in the day-to-day operations of CytoBase. Since CytoBase is physically located at Inspirata's premises there are no transfers of records of personal health information between Inscyte and Inspirata. Inspirata is an agent of Inscyte with respect to the daily operations and maintenance of CytoBase and is not considered to be a third party service provider for the storage of personal health information.

Inscyte requires its agents to comply with its security policies and procedures and designates the Security Officer as being responsible for monitoring and ensuring compliance. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Security Officer to initiate security audits at the prescribed intervals.

Inscyte's security policies also require agents of Inscyte to notify Inscyte at the first reasonable opportunity, in accordance with the Policies and Procedures for Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or any of Inscyte's security policies, procedures and practices.

6. Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices

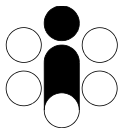
Inscyte Corporation has developed and implemented policies and procedures with respect to the storage, retention, or transfer of records of personal health information on mobile devices. In preparing these policies and procedures Inscyte Corporation has given regard to orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including Order HO-004 and Order HO-007; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation, including Fact Sheet 12: Encrypting Personal Health Information on Mobile Devices, Fact Sheet 14: Wireless Communication Technologies: Safeguarding Privacy and Security and Safeguarding Privacy in a Mobile Workplace.

Inscyte's security policies define a "mobile device" as any portable computing device that can be used to store, retrieve, display and/or allow data to be manipulated or transferred to other devices. As such, "mobile devices" include laptops, notebooks, PDAs, smart phones, tablet computers etc. By contrast, the policies define "portable media" as portable storage media that can only be used in conjunction with a computing device to store and retrieve data. As such, "portable media" includes tapes, diskettes, CDs, DVDs, USB keys, flash memory devices etc. Inscyte makes this distinction since its policies prohibit storing PHI on mobile computing devices, while permitting PHI to be stored on portable media.

Inscyte's policies and procedure prohibit the use of mobile devices for the storage, retention, or transfer of personal health information. Inscyte's policies and procedures permit storing information on portable storage media provided that the files are password protected and encrypted and that the media is stored in a secure location behind at least two physical security checkpoints.

Inscyte requires its agents to comply with its security policies and procedures and designates the Security Officer as being responsible for monitoring and ensuring compliance. The policy and procedures set out the consequences of breach. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Security Officer to initiate security audits at the prescribed intervals.

Inscyte's security policies also require its agents to notify Inscyte at the first reasonable opportunity, in accordance with the Policies and Procedures for Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or any of Inscyte's security policies, procedures and practices.



Where Personal Health Information is Permitted to be Retained on a Mobile Device

Inscyte's security policies expressly prohibit the use of mobile devices for the storage, retention, or transfer of personal health information under any circumstances. As such, Inscyte Corporation has not developed or implemented polices or procedures for the approval/denial of retaining personal health information on a mobile device, or restrictions or conditions on using mobile devices for the storage, retention or transfer of personal health information.

Where Personal Health Information is not Permitted to be Retained on a Mobile Device

Inscyte's security policies expressly prohibit the use of mobile devices for the storage, retention, or transfer of personal health information. However, the security policies permit remote access through a secure virtual private network to systems containing personal health information for the purpose of (a) system maintenance and troubleshooting by authorized staff, and (b) to allow authorized users to access the "CytoBase for Clinicians" online service.

Inscyte Corporation acknowledges that transfers of personal health information to authorized users having access to the "CytoBase for Clinicians" are disclosures under the Act and that the clinicians are not agents of Inscyte. These disclosures are discussed in Part I – Section 12 of this report, however, to provide a more complete picture of the remote access (in this case disclosures as opposed to the more typical uses) to personal health information, which is permitted by Inscyte, we have included a discussion of these transfers as well in the subsections that follow.

Approval Process

Inscyte's policies and procedures stipulate that remote access to systems containing personal information shall only be granted to individual identified persons who have a legitimate need to access the systems and that approval by the Privacy Officer is required, on a person by person basis prior to granting access. The approval process and the policies and procedures for approving/denying access distinguish between (a) technical support staff of Inspirata that require remote access for routine maintenance and troubleshooting activities, and (b) physicians and nurse practitioners in Ontario who wish to use the "CytoBase for Clinicians" online service in their practice.

In the case of technical support staff, the policies state that it is the responsibility of the Security Officer to approve remote access for a limited number of individuals to support the CytoBase system and maintain its availability. The policies state that the minimum criteria for approving remote access for technical support staff are:

a) The agent has completed his/her probationary period of employment.
b) The agent is competent and required to support CytoBase
c) The agent has executed a signed and witnessed Personal Health Information Confidentiality and Non-Disclosure Agreement.

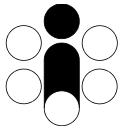
d) The agent has received privacy & security awareness training.

The policies and procedures also require that remote access accounts and passwords be issued in accordance with Inscyte's policies and procedures regarding account names and passwords. The policies further stipulate that all individuals having remote access shall be logged in Inscyte's *Log of Accounts Having Access to PHI* –a perpetual log of individuals' access accounts to computer networks, applications, databases and other secured resources that contain personal health information. The log is maintained in Inscyte's privacy document archives and contains:

a) The full name of the individual to whom the account was granted
b) The account name
c) The resource to which the account applies (e.g. computer/network name, application name, database name or ID etc.)
d) The access level restriction (if any)
e) The reason the account was created
f) The date the account was activated
g) The name of the administrator who created the account
h) The name of the person who authorized the account
i) The status of the account (active, decommissioned, etc.)
j) The date the account was decommissioned
k) The name of the administrator who decommissioned the account
l) The reason for decommissioning the account

In the case of physicians and/or nurse practitioners in Ontario who wish to use the "CytoBase for Clinicians" online service, Inscyte's policies and procedures require that a formal application, authentication, and approval process be followed, comprised of the following:

1. The applicant must fill out Inscyte's standard *CytoBase for Clinicians Account Application Form* (available on paper or downloadable from Inscyte's website) which captures:
    a. Applicants name and job title
    b. Professional designation
    c. Associated healthcare institution or place of work
    d. Address and telephone contact information
    e. Email address
    f. Reason for requesting an account
    g. Agreement to Privacy and Confidentiality "terms of Use" restrictions
2. The form must be signed and dated and delivered to Inscyte's agent Inspirata together with the following supporting documentation:
    a. The applicant's professional license number and licensing body (e.g. CPSO)
    b. A copy of the applicant's current photo ID (e.g. driver's license or passport)



3. The application is reviewed by designated staff of Inscyte's agent Inspirata and the identity and professional standing of the applicant is verified by contacting the applicant's licensing body.
4. After review, it is the responsibility of the Privacy Officer of Inscyte to approve/deny the application and inform the applicant of the decision via email or mail.

The policies set out the requirements and criteria that must be satisfied in order to approve an application to use the "CytoBase for Clinicians" online service as follows:

a) The applicant must be either a licensed physician, nurse-practitioner, or midwife in the province of Ontario.
b) The applicant must be in good standing with his/her professional licensing body.
c) The applicant must be currently in active practice in the province of Ontario.
d) The applicant has demonstrated that in the course of practice he/she has a reasonable and legitimate need to access cervical cancer screening test results on his/her patients and that other information, namely de-identified and/or aggregate information, will not serve the identified purpose.
e) The applicant has indicated that he/she shall comply with the Terms of Use of "CytoBase for Clinicians" and to protect the Privacy and Confidentiality of the information therein.

Inscyte's policies and procedures state that access accounts to "CytoBase for Clinicians" shall expire on an annual basis (from date of issue) and that applicants must re-apply each subsequent year using the process described above. Inscyte's policies and procedures require copies of all applications and approval/denial decisions to be retained in Inscyte's privacy document archives in perpetuity.

Conditions or Restrictions on the Remote Access to Personal Health Information

Inscyte's security policies restrict remote access to personal health information to a few selected technical support persons and approved users of CytoBase for Clinicians. The policies state that remote access to personal health information shall not be granted if other information, namely aggregate or de-identified information shall serve the purpose. Specifically, the policies require technical support staff not to access personal health information whilst performing troubleshooting or maintenance work unless such access is absolutely necessary.

The policy and procedures also set out the administrative, technical, and physical safeguards that must be implemented in providing remote access to technical support staff and online access to "CytoBase for Clinicians". In the case of support staff, access is restricted by multiple sets of account ID and password under a "defense in depth" strategy that requires authentication on successive levels of system access, ranging from remote access to Inspirata's network, access to a specific workstation, access to a specific server, database and so on.

In the case of "CytoBase for Clinicians" online application, a transport layer security server certificate is used to encrypt the connection between the server and the user's browser. The application server communicates with the CytoBase database server through a secondary firewall using an internal non-standard port and an encrypted database server account and password acting as a connection pool. The "CytoBase for Clinicians" application authenticates users via a unique application account ID and password combination for each user. These user accounts and passwords are application-controlled aliases and cannot be used to access the CytoBase database or server directly. All accounts and passwords are required to comply with Inscyte's policies regarding account password composition rules and expiry, de-activation and renewal protocols.

7. Policy and Procedures for Secure Transfer of Records of Personal Health Information

Inscyte Corporation has developed and implemented policies and procedures with respect to the secure transfer of records of personal health information in paper and electronic format.

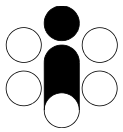
The policies and procedures require records of personal health information to be transferred in a secure manner and set out the methods of transferring records of personal health information and the precautions to be taken depending on whether the information is on paper, portable media, mobile devices (prohibited), email, or computer network transfer. Inscyte's policy and procedures require its agents to use the prescribed methods of transferring records of personal health information and prohibit the use of other methods.

In approving methods and security controls in the secure transfer of personal health information Inscyte Corporation takes into consideration:

- Orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including but not limited to Order HO-004 (stolen laptop) and Order HO-007 (lost USB memory stick);
- Guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario, including Privacy Protection Principles for Electronic Mail Systems and Guidelines on Facsimile Transmission Security; and
- Evolving privacy and security standards and best practices.

In the case of paper-based records, Inscyte's policy requires that the following precautions be applied:

(a) The paper-based records shall be enclosed in a sealed envelope or box (package).
(b) The package(s) shall identify the individual recipient and sender of the information.
(c) The package(s) shall identify the date when the records were sealed.



(d) The package(s) should be labeled to clearly describe that it contains personal health information and the nature of the content.
(e) The package(s) shall be stored in secure premises behind at least two physical security checkpoints before being handed over to couriers for transport.

Furthermore, the policies state that paper-based records of personal health information may not be transported by federal post. Paper-based records shall be transported via commercial bonded courier, by couriers of participating health information custodians (laboratories) of CytoBase, or by the designated staff of either the sender or recipient.

In the case of portable media (e.g. CD's, tapes, USB drives, Flash memory devices) the policies require the following precautions to be applied:

(a) Files on portable media that contain personal health information shall be encrypted and password protected in accordance with Inscyte's policies for file encryption and password formulation, and
(b) In the case of USB drives or other flash memory devices, the device itself shall be password protected, if possible.
(c) The portable media should be labeled to clearly describe that it contains personal health information and the nature of the content.
(d) The password(s) and/or encryption keys shall not be transferred together with the portable media. Passwords and/or encryption keys shall only be disclosed to the recipient via telephone after confirmation and verification of receipt of the portable media and verification of the identity of the recipient.

Inscyte's policies state that transfers of personal health information on portable media must be approved by the Privacy Officer and governed by existing Data Sharing Agreements executed between Inscyte and the recipient of the data, before the data transfers can take place.

Furthermore, the policies state that personal health information on portable media may not be transported by federal post. Portable media shall be transported via commercial bonded courier, by couriers of participating health information custodians (laboratories) of CytoBase, or by the designated staff of either the sender or recipient.

In the case of mobile devices (e.g. laptops, PDAs, tablets, smart phones etc.) or the use of telephone facsimile, Inscyte's policies expressly prohibit the use of mobile devices or telephone facsimile for the transfer of personal health information.

In the case of email, Inscyte's policies state that email should only be used to transfer personal health information in exceptional circumstances where no reasonable alternative approved method is available (e.g. where time is of the essence). In this case, Inscyte's policies require the

personal health information to be transferred as a file attachment to an email message and not in the body of the message. Further, the policies require that the attached file be encrypted, and password protected in accordance with Inscyte's policies for file encryption and password formulation. Also, the policies state that the password to unlock an encrypted file attachment shall not be communicated to the recipient using email. Rather, it shall be communicated to the recipient personally by telephone allowing the sender to verify the recipient's identity.

In the event that Inscyte or its agent Inspirata receives personal health information via email the policies require that the personal health information received shall be saved to a secure server that is part of the secure PHI network and that the email message and attachment(s) be deleted from the email client and the email server forthwith. It is the responsibility of the Security Officer to monitor and ensure that email systems do not retain personal health information.

In the case of computer network transfer of personal health information, Inscyte's policies require the following safeguards to be applied:

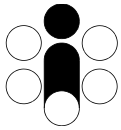
(a) The network connection between sending and receiving systems shall be encrypted and authenticated by implementing a self-managed or third-party public-private key infrastructure (PKI) mechanism with 1024-bit keys as a minimum strength.
(b) Access to the secure network shall require authentication of a unique account ID and password combination (user login) in compliance with Inscyte's policies for issuing account IDs and passwords.

In addition, the policies state that, where possible, files/messages sent over secure networks should be further encrypted at the file/message level using a different encryption mechanism to provide dual layer encryption of personal health information.

The policies and procedures regarding transfer of personal health information also require that transfers of personal health information must be recorded in a *Log of PHI Transfers* containing at minimum:

(a) The date of the transfer
(b) The mode of transfer (paper, portable media, network)
(c) The name of the sender and recipient
(d) The nature of the information transferred
(e) The quantum of personal health information involved (i.e. a count or estimate of the number of person-records involved).
(f) A confirmation of receipt or delivery (date and name of person confirming receipt)

The *Log of PHI transfers* is maintained in perpetuity in Inscyte's privacy document archives. The procedures for transfer of PHI stipulate that the individuals performing the transfers must make



the appropriate entries in the log. It is the responsibility of the Security Officer to ensure that the *Log of PHI Transfers* is being maintained accurate and up to date.

Inscyte requires its agents to comply with its security policies and procedures regarding transfers of personal health information and designates the Security Officer as being responsible for monitoring and ensuring compliance. The policies and procedures also set out the consequences of breach. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Security Officer to initiate security audits at the prescribed intervals.

Inscyte's security policies require its agents to notify Inscyte at the first reasonable opportunity, in accordance with the Policies and Procedures for Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or any of Inscyte's security policies, procedures and practices.

8. Policy and Procedures for Secure Disposal of Records of Personal Health Information

Inscyte Corporation has developed and implemented policies and procedures with respect to the secure destruction and/or disposal of records of personal health information in paper and electronic format to ensure that such records cannot be reasonably recovered or reconstructed after destruction and disposal.

The policy and procedures require records of personal health information to be destroyed and disposed of in a secure manner and define secure destruction and disposal as the transmutation of the media on which personal health information is stored to a form that prevents, using reasonable and foreseeable methods, further access, interpretation, reconstruction or restoration of the information. As such, Inscyte's policies and procedure prescribe specific methods for the destruction and disposal of personal health information on paper, magnetic tapes, optical disks, magnetic disk drives, USB keys & Flash memory devices.

In the case of paper records the policies and procedures state that the personal health information shall be destroyed by cross-cut shredding, pulverization or incineration and further require that printed documents containing personal health information shall not be disposed of in waste baskets, re-cycling bins, or any other normal waste disposal methods.

In the case of personal health information stored on portable media (e.g. CDs, DVDs, tapes and USB keys or Flash memory devices), the policies state that in the event that the portable media are to be reused, the files containing personal health information shall be deleted from the media using a method the renders the files un-recoverable, such as commercial file shredding software

or re-formatting the storage media. In the event that the portable media are not to be reused or it is not possible to delete information from the media the policies require the media to be destroyed in a manner rendering it unusable and then discarded. To this end, the policies and procedures set out acceptable methods for destroying various types of media as follows.

For tapes, diskettes, DVDs or CDs an acceptable procedure is to de-gauss magnetic media, remove or black out any information printed on the tape, diskette, CD or DVD that describes the contents, author, owner, sender or recipient of the data. Make deep scratches into the optical surface of CDs or DVDs. Cut or tear the media into at least five random pieces and deform the pieces. Dispose of the pieces in at least two physically separate disposal locations.

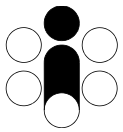
For electronic memory devices, such as USB keys or flash memory an acceptable procedure is to de-gauss the media if possible, then crush or pulverize the device using a hammer or other implement so that it is in at least five (5) pieces and to dispose of the pieces in at least two physically separate disposal locations.

For internal disk drives, an acceptable procedure is to remove the disk(s) from the computer housing. De-gauss the disks. Open the disk chassis and remove the platters, by force, if necessary. Then deform the platters to destroy alignment.

In addressing the precise method by which records of personal health information in paper and electronic format must be securely destroyed and disposed of, has given regard to the Act and its regulation; and orders issued by the Information and Privacy Commissioner of Ontario, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation, including Fact Sheet 10: Secure Destruction of Personal Information.

Inscyte's policies and procedures require that personal health information intended for destruction in paper or electronic formats to be stored in a secure clearly marked and locked physical location, behind at least two physical security checkpoints, in an area designated for the secure retention of records pending destruction and disposal and segregated from records intended for recycling. It is the responsibility of the Security Officer to ensuring the secure storage of records of personal health information pending their secure disposal.

Inscyte's policies and procedures state that in the event that records of personal health information are to be securely disposed of by a designated agent, who is not a third-party service provider, Inscyte will provide to the agent a written instruction setting out the nature of the information to be disposed of, stipulate acceptable methods of destruction/disposal, and set out the time frame in which the agent is to dispose of the information. It is the responsibility of the Privacy Officer to issue the instruction letter to the agent. Further, Inscyte's policies require the



agent to return to Inscyte a written and signed confirmation letter within the prescribed time frame:

- Identifying the records of personal health information to be securely disposed of.
- Confirming the secure disposal of the records of personal health information.
- Setting out the date, time and method of secure disposal employed; and
- Bearing the name and signature of the agent(s) who performed the secure disposal.

In the event that records of personal health information on paper or electronic media will be securely disposed of or destroyed by a third-party service provider, Inscyte's policies require:

a) Using a service provider that is accredited by an industrial trade association, such as the National Association for Information Destruction, or willing to commit to upholding its principles, including undergoing independent audits.
b) The service provider to issue a certificate of destruction (as described above) in each service instance.
c) That a copy of the certificate of destruction be retained in Inscyte's privacy document archives in perpetuity.
d) That transfer of paper or electronic media bearing personal health information and intended for destruction between Inscyte and the service provider shall be conducted in accordance with Inscyte's policies and procedures for the secure transfer of personal health information.

Inscyte's policies state that it is the responsibility of the Security Officer to ensure compliance with this policy when third-party service providers are engaged for the destruction and disposal of paper or electronic media containing personal health information.

Further, where a third party service provider is retained to securely dispose of records of personal health information, Inscyte's policy requires that a written agreement be executed with the third party service provider containing the relevant language from Inscyte's Template Agreement for Third Party Service Providers, and identifies the Security Officer as responsible for ensuring that the agreement has been executed prior to the transfer of records of personal health information for secure disposal.

The policy and procedures require that transfers of paper or electronic media containing personal health information slated for destruction and disposal be tracked in a *Log of PHI Destruction and Disposal*, which is to be retained in Inscyte's privacy document archives and contain the following information at minimum:

a) The name of the service provider
b) The nature of the media and information to be disposed of or destroyed

c) The date and time the paper or electronic media were transferred for disposal
d) The name of the individual who transferred the media to the service provider
e) The date by which a certificate of destruction is expected
f) The date the certificate of destruction was received

The policies state that it is the responsibility of the Security Officer to ensure the *Log of PHI Destruction and Disposal* is maintained up-to-date and accurate, to track the expected receipt of certificates of destruction.

In the event that a certificate of destruction is overdue, the policies and procedures require the Security Officer to inform the Privacy Officer that a certificate is overdue and to send a reminder notice to the service provider to obtain the certificate forthwith. If the service provider fails to provide the certificate of destruction after the reminder notice is sent, the policies require the issue shall to be referred to the President of Inscyte and brought before the Board of Directors to determine the actions to be taken in resolving the issue.

Inscyte requires its agents to comply with its security policies and procedures regarding the secure disposal of records personal health information and designates the Security Officer as being responsible for monitoring and ensuring compliance. The policy and procedures also set out the consequences of breach. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Security Officer to initiate security audits at the prescribed intervals.

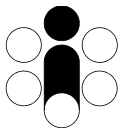
Inscyte's security policies require its agents to notify Inscyte at the first reasonable opportunity, in accordance with the Policies and Procedures for Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or any of Inscyte's security policies, procedures and practices.

9. Policy and Procedures Relating to Passwords

Inscyte Corporation has developed and implemented policies and procedures with respect to passwords for authentication and passwords for access to information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by Inscyte Corporation.

The policies for issuing access accounts and passwords stipulate the following general requirements:

a) Minimum length of passwords shall be ten (10) characters
b) Passwords shall be composed of alphabetic, numeric, and non-alphanumeric characters
c) Passwords shall be of mixed upper/lower case



d) Passwords shall expire at maximum on a 90-day cycle
e) A user's previous two passwords cannot be re-used when changing passwords
f) Except when originally issued passwords cannot be the same as account names
g) A user must change his/her password upon first use of a newly issued account
h) Each combination of account name and password shall be unique
i) Account names cannot be re-used for different individuals

The policies state that the above requirements shall be implemented to the maximum extent possible; recognizing that not all software, computer applications and equipment may support all of the above requirements.

The policies further state that whenever possible, three (3) successive failed attempts at authenticating a user's account ID and password combination should automatically disable the account, record the event in a failed login log, and alert system administrators about the event. Upon discovery of a failed login event, Inscyte's policies stipulate that an investigation shall be undertaken to determine if a breach of security or potential breach has occurred. The policies state that it is the responsibility of the Security Officer to ensure an investigation is carried out.

Inscyte's security policies require that all computer workstations that can access personal health information implement a maximum ten (10) minute idle timeout that locks the workstation and requires re-entry of a user's password to resume work.

Further, Inscyte's security policies in respect of passwords set out that each individual must keep his/her password secret and not share it with any other individual, that passwords should not be comprised of an individual's postal code, date of birth, vehicle license plate number or other publicly available information related to the individual. In the event that an individual suspects his/her account/password has or may have been compromised, the policies require the individual to report the incident to the Security Officer, and that the account/password be de-activated and a new account/password issued.

Inscyte's policies also set out the administrative procedures for requesting and issuing account names and passwords for access to systems containing personal health information. Inscyte's policies and procedures stipulate that access shall only be granted to agents of Inscyte and that approval by the Privacy Officer is required prior to granting access. The policies state that the minimum criteria for approving individual access accounts are:

a) The agent has a legitimate need to access systems containing personal health information
b) The agent has completed his/her probationary period of employment.
c) The agent has executed a signed and witnessed Personal Health Information Confidentiality and Non-Disclosure Agreement.

d) The agent has received privacy & security awareness training.

The policies further stipulate that all individuals having access accounts shall be logged in Inscyte's *Log of Accounts Having Access to PHI* –a perpetual log of individuals' access accounts to computer networks, applications, databases and other secured resources that contain personal health information.

In developing its policies and procedures regarding passwords and access accounts, Inscyte gives regard to orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation; guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario; and with evolving privacy and security standards and best practices.

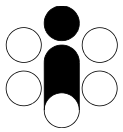
Inscyte requires its agents to comply with its security policies and procedures regarding passwords and access accounts and designates the Security Officer as being responsible for monitoring and ensuring compliance. The policies and procedures set out the consequences of breach. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Security Officer to initiate security audits at the prescribed intervals.

Inscyte's security policy requires its agents to notify Inscyte at the first reasonable opportunity, in accordance with the Policies and Procedures for Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or any of Inscyte's security policies, procedures and practices.

10. Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs

Inscyte Corporation has developed and implemented policies and procedures for maintaining and reviewing system control and audit logs with respect to CytoBase. The policies require that all information systems, technologies, applications and programs related to CytoBase and involving personal health information have the functionality to log access, use, modification and disclosure of personal health information. As such, the policies require the following logs to be maintained and specify Inspirata as agent of Inscyte responsible for ensuring that these logs are maintained and reviewed to monitor compliance with the policies.

1) Individual user connection log
2) Data modification audit log
3) Data disclosure audit log
4) Network transaction log



5) Firewall activity logs
6) Web server activity logs

These logs are maintained by automated software processes built into the CytoBase system.

The *Individual User Connection Log* is a CytoBase application log and contains the following information:

- A unique connection ID (system generated)
- The account ID name making the connection (corresponds to a user)
- The network/computer name from which the connection was made
- The date/time of connection start
- The date/time of disconnect
- The nature of the disconnect (normal, timeout, or dropped)

Entries are added to this log whenever a user (or software process) connects to the CytoBase database, explicitly disconnects, or when an idle connection expires. The absence of a disconnect timestamp indicates a dropped connection. This log is retained in perpetuity. It is located on the CytoBase database server in Inspirata's secure datacenter and periodically archived to portable media, which are stored in secured premises behind at least two physical checkpoints.

The *Data Modification Log* is a CytoBase application log and contains the following information:

- The date/time of data modification
- The account ID making the modification (corresponds to a user)
- The affected patient ID (unique key to a patient record)
- The affected data entity ID (e.g. report ID, follow-up entry ID etc.)
- The type of modification action (insert, update or delete)
- The affected field names and new values (for insert and update actions)

Entries are added to this log whenever changes are made to data via the CytoBase data registration system or via administrative applications. This log is retained in perpetuity. It is located on the CytoBase database server in Inspirata's secure datacenter and periodically archived to portable media, which are stored in secured premises behind at least two physical checkpoints.

The *Data Disclosure Log* is a CytoBase application log that contains the following information:

- The date/time of disclosure
- The account ID triggering the disclosure

- The affected patient ID (unique key to a patient)
- The type of disclosure:
    - response to a network query from a laboratory
    - placement on a follow-up letter package
    - linkage to another data source
    - retrieval through an administrative application
- The nature of the information disclosed (e.g. test results, last screening date etc.)

Entries are added to this log whenever CytoBase processes data whether triggered by an automated process or through administrative applications. This log is retained in perpetuity. It is located on the CytoBase database server in Inspirata's secure datacenter and periodically archived to portable media, which are stored in secured premises behind at least two physical checkpoints.

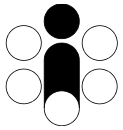
The *Network Transaction Log* records the on-going exchange of information (messages) between CytoBase and participating laboratories and contains the following information:

- The date/time of message receipt/transmission
- A unique message ID (system generated)
- The type of message (report submission, query request, query response etc.)
- The IDs of sending and receiving systems
- The success/failure of the transaction
- A copy of the raw message content

Entries are added to this log by the CytoBase network listener processes as messages are received and sent. This log is retained in perpetuity. It is located on the network communications server in Inspirata's secure datacenter and periodically archived to portable media, which are stored in secured premises behind at least two physical checkpoints.

The *Firewall Activity Logs* record the traffic between computers connecting to the CytoBase system externally (via the Internet) and internally (on Inspirata's private network). These logs contain the following information.

- The date/time of connection
- The IP address of the computer making the connection
- The firewall port number of the connection
- The success/failure of the connection
- The inbound/outbound traffic count (in bytes)



Entries to these logs are made automatically by the firewall systems. These logs are reviewed and archived on a regular basis. The purpose of the reviews is to detect network intrusion attempts. Archived logs are stored in Inspirata's datacenter. These logs do not contain PHI.

The *Web Server Activity Log* records hypertext transfer protocol requests and responses to Inscyte Corporation's public website and the CytoBase for Clinicians online service. This log contains the following information:

- The IP address or URI of the computer making the request
- The date/time of the request
- The request command
- The return/response code for the request

Entries into this log are made automatically by the web application server software. This log does not contain personal health information. This log is reviewed on a regular basis to monitor web server activities and detect intrusion attempts and/or various types of Internet attacks.

Inscyte's policies also require restricting access to system control and audit logs to a limited number of individuals (system support personnel and authorized users of CytoBase administrative applications only) and prohibit these individuals from modifying, deleting audit log data or tampering with the automated audit logging processes.

Inscyte's policies and procedures stipulate that in order to render system control and audit logs immutable, the logs must be archived to read-only portable media on a regular schedule. The portable media must be treated as personal health information and stored in secured locations behind at least two physical security checkpoints. It is the responsibility of the Security Officer to ensure that system control and audit logs are archived at appropriate intervals and stored in secured locations. The policies further prohibit the destruction of archived system control and audit logs.

Inscyte's policies require that CytoBase system control and audit logs be monitored on an on-going basis using automated real-time monitoring software, to detect and trigger alerts in the event of unusual activity or degradation in system performance. It is the responsibility of the Security Officer to ensure that the automated monitoring processes are enabled and in operation on a continuous basis. Inscyte does not have a specific policy for documenting the results of these reviews, however, Inscyte's policies require that all agents of Inscyte be vigilant of circumstances that may indicate a breach or attempted breach of security. As such, if in the course of reviewing system control and audit logs evidence is found that a breach or attempted breach of security may have occurred, the policies require investigating the breach in accordance with Inscyte's policies and procedures in respect of security breach management that state if

there is also cause to believe that a privacy breach may have occurred, Inscyte's policies and procedures for privacy breach management shall take effect as well.

Inscyte requires its agents to comply with its security policies and procedures regarding the maintenance and review of system control and audit logs and designates the Security Officer as being responsible for monitoring and ensuring compliance. The policy and procedures set out the consequences of breach. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Security Officer to initiate security audits at the prescribed intervals.

Inscyte's security policies also require agents of Inscyte to notify Inscyte at the first reasonable opportunity, in accordance with the Policies and Procedures for Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or any of Inscyte's security policies, procedures and practices.

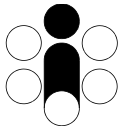
11. Policy and Procedures for Patch Management

Inscyte Corporation has policies and procedures in place for patch management. The objective of Inscyte Corporation's patch management program is to create a consistently configured environment that is secure against known vulnerabilities in operating systems, network devices, and application software.

Inscyte's patch management policy designates the Security Officer as having overall responsibility for the patch management program, and designates its Agent Inspirata as responsible for keeping up to date on newly released patches and security issues that affect the systems and applications deployed in the CytoBase environment. The policy also designates Inspirata to be responsible for alerting administrators and users of security issues and performing required updates to the operating systems, network devices, and application software.

Inscyte's patch management policy requires it Agent Inspirata to maintain a comprehensive and accurate asset inventory to be used to determine whether all existing systems are accounted for when researching and applying patches.

Inscyte's patch management policy categorizes patches as being critical, routine, or low priority and sets out the schedule for implementing patches depending on priority. Inscyte's policy states that critical patches are to be applied at the earliest possible opportunity since becoming available; that routine patches be applied no later than three months from availability; and that low priority patches are to be implemented no later than six months of becoming available. Inscyte's policy states that patch priority is to be assessed based on vendor-reported severity (high, medium, low) and the existence of a known exploit or other malicious code that uses the



vulnerability being patched as an attack vector. For example, a high-risk vulnerability coupled with a known existing exploit qualifies as a critical priority patch.

Inscyte's policy sets out the criteria for determining whether a patch should be implemented. The policy states that all vendor-recommended patches should be applied in accordance with the prioritization and scheduling policy. The policy states that patches can be applied without express authorization of Inscyte unless there is reason to believe that a patch will significantly degrade the performance of CytoBase, the strength of its security controls, availability or functionality, or require additional funding to implement. In this case, the policy states that it is the responsibility of its Agent Inspirata to bring the issue to the attention of the Security Officer and the Board of Inscyte for further discussion, recommendations, review, and approval.

In the event that a determination is made that a patch should not be implemented, Inscyte's policies require its Agent Inspirata to document the determination, including:

- A description of the patch
- The date the patch became available
- The severity/importance of the patch
- The affected software or hardware components
- The rationale for not implementing the patch

Inscyte's policy also addresses patch testing. The policy states that patches to enabling software and/or firmware published by established vendors (such as Microsoft, Oracle, Cisco) do not require testing provided that there is a rollback mechanism in place to revert the patch in the event it causes unexpected system behavior. The policy states that patches to user application software must be tested prior to release into the production environment and designates its Agent Inspirata as being responsible for the testing. The policy states that the time frame for testing is to be in accordance with the policy for prioritization and scheduling.

The policy also requires Inspirata to maintain a complete and accurate Configuration Change Log that is used to manage changes and record all changes made to CytoBase system software and hardware components over time. The policy requires the following information to be recorded in the Configuration Change Log:

- A description of the patch
- The date the patch became available
- The severity/importance of the patch
- The affected software or hardware component
- The date the patch was tested (if testing was required)
- The agent(s)/personnel that tested the patch (if testing was required)

- The date the patch was implemented in production
- The agent(s)/personnel that implemented the patch

Inscyte requires its agents to comply with its security policies and procedures regarding patch management and designates the Security Officer as being responsible for monitoring and ensuring compliance. The policy and procedures set out the consequences of breach. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on an ad-hoc basis. It is the responsibility of the Security Officer to initiate security audits at the prescribed intervals.

Inscyte's security policies also require agents of Inscyte to notify Inscyte at the first reasonable opportunity, in accordance with the Policies and Procedures for Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or any of Inscyte's security policies, procedures and practices.

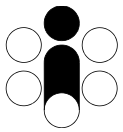
12. Policy and Procedures Related to Change Management

Inscyte's policy for change management designates its agent Inspirata as being responsible for evaluating the necessity and implementing changes to the operational environment of CytoBase as necessary to maintain 7x24 operations and to keep pace with evolving operating system, database, network, security and other supporting technologies.

As Inspirata is the designer and developer of CytoBase, Inscyte's policy delegates authority to Inspirata to implement changes at its sole discretion provided that such changes do not degrade the performance of CytoBase, the strength of its security controls, availability, or its functionality, and that such changes do not require securing additional funding.

In all other cases, the policy requires Inspirata to submit a change request consisting of a description of the change and its rationale, the impact of executing or not executing the change, and a work/cost breakdown and implementation schedule to Inscyte for prior approval. It is the responsibility of the CEO of Inspirata to communicate the change request to Inscyte in writing. It is the responsibility of the President of Inscyte to approve/deny each change request, based on the criteria identified in the policy. The President of Inscyte approves or denies each change request, in writing, and provides reasons for his decision to the CEO of Inspirata.

With respect to the computing infrastructure of CytoBase, it is the responsibility of Inspirata's Operations Manager to evaluate existing infrastructure and plan for upgrades on an on-going basis taking into account obsolescence, maintainability, technological improvements, emerging technologies, and recommendations resulting from privacy and security audits or breach investigations, among other factors.



It is the responsibility of the Operations Manager to bring forward recommendations for changes to the computing infrastructure to Inspirata's Management, and to the President of Inscyte if the changes require Inscyte's approval.

Inscyte's policy does not set out specific criteria on which changes to infrastructure are to be evaluated but require that recommendations be accompanied with a clear rationale describing the benefits of the changes.

Implementation of infrastructure changes are performed in accordance with Inspirata's engineering practices and protocols, which require changes to be tested and verified on non-production systems before being rolled-out to production environments, with provisions for reverting to previous good configurations if required. It is the responsibility of the Operations Manager to monitor and ensure that changes are implemented in accordance with specifications and set schedules. Inspirata's engineering practices and protocols require documentation to be maintained regarding all infrastructure changes, which include the minimum information required by the IPC Manual.

Inscyte's policy requires Inspirata to maintain accurate and up-to-date *Asset Inventory and Configuration Information* documentation for all components of the CytoBase infrastructure, describing each component, component type, its vendor, configuration, and date(s) of installation and/or upgrades, which include the minimum information required by the IPC Manual. This documentation is maintained by Inspirata as part of Inscyte/Inspirata Risk Management and Business Continuity policies and procedures.

Inscyte requires its agents to comply with its security policies and procedures regarding change management and designates the Security Officer as being responsible for monitoring and ensuring compliance. The policy and procedures set out the consequences of breach. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Security Officer to initiate security audits at the prescribed intervals.

Inscyte's security policies also require agents of Inscyte to notify Inscyte at the first reasonable opportunity, in accordance with the Policies and Procedures for Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or any of Inscyte's security policies, procedures and practices.

13. Policy and Procedures for Back-Up and Recovery of Records of Personal Health Information

Inscyte has developed and implemented a policy for the back-up and recovery of personal health information contained in CytoBase. The back-up/recovery policy designates Inscyte's agent

Inspirata as being responsible for all back-up and recovery services. Inscyte Corporation does not use a third-party service provider for back-up and recovery services.

The policy requires that back-ups be performed in such a manner that the complete CytoBase database can be restored with a maximum loss of one week's data. The policy states that back-up media shall be made available to restore the CytoBase system to a good state in the event that an upgrade or change to the computing infrastructure requires reverting to a previous state, the a system failure occurs which requires restoring CytoBase to a last known good state, and in support of Inscyte's disaster recovery strategy.

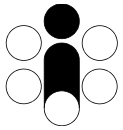
It should be noted that CytoBase is a copy of information emanating from participating laboratories and the loss of up to several weeks of data can be restored by re-playing transmissions from participating laboratories using the Network Transaction Logs residing at the laboratories.

Inscyte's policy requires that a complete back-up be performed on a daily basis to portable media (tapes) labeled with the date and time of the backup. The policy further requires that a log of back-ups be maintained with the date and sign-off by the individual making each day's backup tapes. The policy requires that two sets of tapes be maintained: one on-site and one off-site, and that the tapes must be stored in a secure location behind at least two physical security checkpoints. The policy designates Inspirata's Operations Manager as being responsible for ensuring that daily back-ups are performed in accordance with the policy.

In support of the policy, Inspirata performs full daily backups of CytoBase to tape on a two-week rotation. The back-up is performed by an automated system that incorporates a tape-loader. The daily tapes for the current week are store on-site in a fireproof safe in Inspirata's datacenter. The previous week's set of daily back-ups are stored off-site in a secure location. The weekly tape sets are rotated from week to week.

The policy and procedures also require that restoration tests be performed on a quarterly basis (at minimum) to verify that the back-up tapes are useable. The test requires selecting a back-up tape at random and performing a restore on selected files. It is the responsibility of Inspirata's Operations Manager to ensure that restoration tests are performed and that in the event of a failure, to report the failure to Inspirata's management for resolution and remediation.

Inscyte requires its agents to comply with its security policies and procedures regarding change management and designates the Security Officer as being responsible for monitoring and ensuring compliance. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Security Officer to initiate security audits at the prescribed intervals.



Inscyte's security policies also require agents of Inscyte to notify Inscyte at the first reasonable opportunity, in accordance with the Policies and Procedures for Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or any of Inscyte's security policies, procedures and practices.

14. Policy and Procedures on the Acceptable Use of Technology

Inscyte Corporation has developed and implemented a policy regarding the acceptable use of information systems, technologies, equipment, resources, applications, and programs insofar as the handling of personal health information is concerned. The policy addresses prohibited uses of technologies only. All other uses are permitted, and no policy exists for uses that are permitted only with prior approval.

The policy expressly prohibits the following:

1. Wireless access points to computer networks containing PHI are prohibited
2. Sending PHI in open text email messages is prohibited
3. Printing of material containing PHI in unsecured premises is prohibited
4. Storing PHI on portable computing devices is prohibited
5. Sending PHI via facsimile is prohibited

The policy also sets out acceptable practices for the implementation of browser-based user applications that provide access to personal health information via the Internet, including the requirements for strong third-party server security & encryption certificates, disabling access to remote server management consoles, disabling non-required ports on firewalls and disabling un-needed Internet communication protocols such as Telnet and Secure Shell on all such public-facing systems.

Inscyte requires its agents to comply with its security policies and procedures regarding acceptable use of technology and designates the Security Officer as being responsible for monitoring and ensuring compliance. The policy and procedures set out the consequences of breach. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Security Officer to initiate security audits at the prescribed intervals.

Inscyte's security policies also require agents of Inscyte to notify Inscyte at the first reasonable opportunity, in accordance with the Policies and Procedures for Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or any of Inscyte's security policies, procedures and practices.

15. Policy and Procedures In Respect of Security Audits

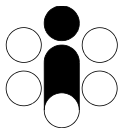
Inscyte Corporation's policies require that a security audit be performed on an annual basis to assess security risks and whether current security policies and controls are adequate to mitigate the identified risks. In practice, Inscyte's Agent Inspirata, reviews security policies, controls, and emerging risks on a weekly basis at routine weekly operations department review meetings.

Inscyte's policy states that the purposes of the security audit is to ensure that its information security program adequately addresses the preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required) of personal health information and business critical information; and to ensure that the information security program complies with all applicable legislation and keeps pace with emerging best practices.

Inscyte's policies state that it is the responsibility of the Privacy Officer to initiate an annual security audit and that it is the responsibility of the Security Officer to conduct and report on the findings of the audit.

Inscyte's annual security audits are conducted in conformance with ISO/IEC 27002 Information Security Standards. Accordingly, the policy identifies the following subject matter areas to be reviewed and sets out general instructions for doing so as follows:

1. Threat Risk assessments (TRAs)
    a. Review *Threat Risk Assessments* to assess completeness and accuracy
    b. Assess adequacy of response to previous TRA recommendations (if any)
    c. Assess if new TRAs are required to align with changing assets and/or processes
2. Vulnerability Assessment – emerging threats
3. Security policy - management direction
    a. Review current strategic objectives regarding information security
    b. Assess adequacy/alignment of strategic objectives
4. Organization of information security - governance of information security
    a. Review governance structure
    b. Assess adequacy and effectiveness of governance structure
5. Asset management - inventory and classification of information assets
    a. Review *Asset Inventory and Configuration Information* to ascertain accuracy and completeness
6. Human resources security – access rights of agents joining, moving and leaving the organization



   a. Review the *Log of Individuals Having Access to Premises* to ascertain accuracy and completeness
   b. Assess adequacy of access rights and roles for each individual
7. Physical and environmental security - protection of the computer facilities and premises where personal health information is stored
   a. Inspect physical security checkpoints and entry logs to ascertain functionality and completeness
   b. Assess adequacy of physical security controls
   c. Inspect environmental controls to ascertain functionality
   d. Assess adequacy of environmental controls
8. Communications and operations management - management of technical security controls in systems and networks
   a. Review technical security controls in servers, networks, workstations etc.
   b. Review system access and control logs to determine completeness and functionality
   c. Review emerging trends, technologies and best practices
   d. Assess adequacy of technical security controls
9. Access control - restriction of access rights to networks, systems, applications, functions and data
   a. Review the *Log of Individuals Accounts Having Access to PHI* to ascertain accuracy and completeness
   b. Assess adequacy of access rights and roles for each individual
   c. Assess adequacy of application security controls
10. Information systems acquisition, development, and maintenance - building security into applications
   a. Review all technical security controls in the computing infrastructure
   b. Identify differences in technical security controls from one checkpoint to another
   c. Assess adequacy and consistency of checkpoint security controls
   d. Assess potential weaknesses or obsolescence of technical security controls
   e. Review all back-up/restore and system availability controls
   f. Review outages (planned or unplanned) and assess adequacy of response
   g. Assess adequacy of system availability controls
11. Information security incident management - anticipating and responding appropriately to information security breaches
   a. Review *Log of Security Breaches* to assess completeness and accuracy
   b. Assess adequacy of response to security breaches
   c. Analyze security breaches and recommend solutions to prevent recurrence
12. Business continuity management - protecting, maintaining and recovering business-critical processes and systems
   a. Review the current *Disaster Recovery Plan* for accuracy and completeness

   b. Assess adequacy of the disaster recovery plan with respect to current assets and operations
13. Compliance - ensuring conformance with security policies and procedures, standards, laws, and regulations
   a. Review security policies and procedures; emerging standards and best practices; laws and regulations
   b. Assess compliance with above

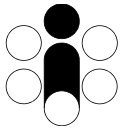
With respect to technical security controls in systems and networks, and access controls to networks, systems, applications, functions and data, the policy and procedures provide guidelines for performing penetration testing and ethical hacks to assess the strength and adequacy of these security controls.

All of the above subject matter areas are addressed in annual security audits, however the policies permit specific areas to be addressed at any time if there is reason to believe a deficiency exists in the security program or in the event of a breach or suspected breach of security has occurred. It is the responsibility of the Privacy Officer to determine if an audit of a specific subject matter area is required under such circumstances.

The policies require that a *Security Audit Report* to be prepared for each subject matter area identifying the subject matter, the date the audit was started and completed, the activities performed, the names of the individuals carrying out the audit, the findings and resulting recommendations for changes (if any) and the proposed manner in which the recommendations shall be addressed. The policies require that these reports are to be retained in perpetuity in the *Log of Security Audits* in Inscyte's privacy document archives.

The policies further require that each *Security Audit Report* must be reviewed and approved by the Security Officer and a copy provide to the Privacy Officer and the President of Inscyte. It is the responsibility of the Security Officer to track any recommendations for changes resulting from security audits; to ensure that the recommendations are summarized in the *Consolidated Log of Recommendations*, and to determine the schedule upon which recommendations shall be acted upon giving regard to the nature and urgency of the recommended changes. The policies require that recommended changes resulting from security audits are to be implemented in accordance with Inscyte's policies and procedures for change management and/or its policies regarding patch management.

The policy further requires that a *Log of Security Audits* be maintained in perpetuity within Inscyte's privacy document archives and designates the Security Officer as being responsible for maintaining the log and for tracking that the recommendations arising from security audits are addressed within the specified time frame.



Inscyte's policy and procedures regarding security audits also require agents responsible for conducting security audits to notify Inscyte, at the first reasonable opportunity, of an information security breach or suspected security breach in accordance with the Policy and Procedures for Information Security Breach Management and of a privacy breach or suspected privacy breach in accordance with the Policy and Procedures for Privacy Breach Management.

16. Log of Security Audits

Inscyte Corporation maintains a *Log of Security Audits* that have been completed. The log contains a summary of each *Security Audit Report* identifying the subject matter are that was audited, the date the audit was started and completed, the activities performed, the names of the individuals carrying out the audit, the findings and resulting recommendations for changes (if any) and the proposed manner in which the recommendations shall be addressed.

Inscyte's policies also require that recommendations from security audits be recorded in its *Consolidated Log of Recommendations* for tracking and work scheduling purposes.

17. Policy and Procedures for Information Security Breach Management

Inscyte Corporation has developed and implemented policies and procedures to address the identification, reporting, containment, notification, investigation, and remediation of security breaches. The policies define a "breach of security" as:

a) An unauthorized person gaining access to, or attempting to gain access to, secured premises or secured information, by any means whatsoever.
b) An act that compromises the confidentiality, integrity (accuracy and completeness), or availability of secured information.
c) A contravention of Inscyte's security policies and procedures.

Inscyte's policy does not differentiate between a "security breach" and "information security breach". Rather, the policies state that a breach of security occurs in the above circumstances regardless of the consequences of the breach, and in the event that there is reasonable cause to believe that personal health information has been disclosed to unauthorized parties, or is likely to be disclosed as a consequence of the security breach, Inscyte's policies and procedures for privacy breach management shall also come into effect.

In addition to providing a definition of a breach of security, Inscyte's policies further state that a breach of security occurs whenever a person has gained, or attempts to gain, unauthorized access to secured premises or secured information; that a breach of security may be reported via a complaint or challenge to Inscyte's or its agent's compliance with these policies and procedures filed by a third party; and that a breach of security may be self-identified by an agent of Inscyte through the course of everyday work signaled by the discovery that (without limitation):

a) A physical security control has been damaged, disabled or tampered with
b) A key or pass card is found in a suspicious location
c) A security log (computer network access logs, application access logs, internet activity logs etc.) contains information indicative that unauthorized access has been attempted.
d) A computer security control behaves erratically or is disabled
e) A computer system is disabled or behaves erratically
f) Computer files are missing or corrupted
g) A database system is corrupted
h) Unexpected loss of availability of a computer system or data

The policies state that upon discovery of a breach or suspected breach of security, the party discovering the breach shall immediately report the incident to the Privacy Officer and Security Officer of Inscyte either verbally or by email. The policies include the contact information for the Privacy and Security Officers.

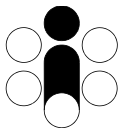
Inscyte's policies and procedures for security breach management further set out the actions to be taken after discovery of a breach or suspected breach of security.

The policies require that the reported incident be immediately assessed to determine if a breach of security has in fact occurred and to further determine if a breach of privacy has also occurred, or is likely to occur as a result of the security breach. It is the responsibility of the Security Officer to ensure that this assessment is performed. The policies state that if there is reasonable cause to believe that personal health information has been disclosed to unauthorized parties, or is likely to be disclosed as a consequence of the security breach, then it is the responsibility of the Security Officer to immediately notify the Privacy Officer about the breach, at which time Inscyte's policies and procedures for privacy breach management also take effect.

The policies then require that a confirmed breach of security be contained by taking all necessary actions to secure the premises and/or information systems affected by the breach, including suspending access to authorized individuals, recovering access keys, pass cards, re-setting access codes and accounts, taking affected computer systems off-line and so forth, in order to mitigate against further security breaches of the same or similar nature It is the responsibility of the Security Officer to ensure that these actions are taken as quickly as possible and to determine whether the security breach has been effectively contained or whether further containment measures are necessary.

The policies also require that each incident of security breach be documented using Inscyte's standard *Security Breach Report* which contains the following information at minimum:

a) Incident report number (unique for each incident)



b) The incident report date
c) The name/title of the person(s) who discovered/reported the breach security
d) The name/title of the person(s) who investigated the breach of security
e) The date/time of the breach (or estimate thereof)
f) The evidence that lead to the discovery of the breach of security
g) likelihood and/or evidence that a breach of privacy also occurred (if any)
h) Containment procedures (what was done to contain the breach, when and by whom)
i) Suspected perpetrator the breach (if known)
j) The motivation/cause for the breach (or suspected motivation/cause)
k) Description of security controls that were compromised
l) Description of how the security controls were compromised
m) Recommendations for changes and mitigating strategies
n) The agent(s) responsible for implementing the recommendations
o) The date each recommendation is expected to be addressed
p) The manner in which each recommendation is expected to be addressed
q) Sign-off/approval name, title and date

It is the responsibility of the Security Officer to delegate work to appropriate staff and ensure that an investigation is carried out and report is completed as quickly as possible and no later than 30 days following a breach of security. The policies require that the *Security Breach Report* be provided to the Privacy Officer and the President of Inscyte for review and final approval. The policies further require that all Security Breach Reports be retained in perpetuity in Inscyte's privacy document archives.

In the event that a breach of security includes a breach of privacy, Inscyte's policies and procedures for privacy breach management come into effect and require the Privacy Officer to immediately notify the President of Inscyte about the breach, either verbally or by email. The policies state that is subsequently the responsibility of the President of Inscyte to notify, at the first reasonable opportunity, the health information custodians or other organizations that disclosed the personal health information to Inscyte Corporation and advise them of the extent of the breach; the nature of the personal health information at issue; the measures taken to contain the breach; and any further actions that will be undertaken with respect to the breach.

Inscyte's policies and procedures require that recommendations for changes and mitigating strategies emanating from investigations of security breaches also be recorded in the *Consolidated Log of Recommendations* citing the Security Breach Report number as the source of the recommendations and specifying the actions to be taken to implement the recommendations, the personnel responsible for carrying out the actions, and the target date(s) of completion. The policies designate the Security Officer as responsible for logging the recommendations; delegating work to address the recommendations; establishing timelines to

address the recommendations; and for monitoring and ensuring that the recommendations are implemented within the stated timelines.

The policy and procedures require that upon completion of recommended changes, all affected documents, such as the *Asset Inventory and Configuration Information, Log of Individuals Having Access to PHI, Log of Individuals Having Access to Premises,* and so forth are updated to reflect the implemented changes and that the *Consolidated Log of Recommendations* is updated to reflect the completion of the changes, the date of completion and the name/title of the person confirming the completion. The policies designate the Security Officer as being responsible to ensure that the related documentation is up-to-date and accurate.

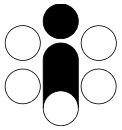
Further, Inscyte's policies and procedures require that a *Log of Security Breaches* be maintained and identify the Security Officer as responsible for maintaining the log and for tracking that the recommendations arising from the investigation of security breaches are addressed within the identified timelines. The policies require that *Security Breach Reports* in the *Log of Security Breaches* be maintained in perpetuity in Inscyte's privacy document archives.

Inscyte requires its agents to comply with its security policies and procedures regarding security breach management and designates the Security Officer as being responsible for monitoring and ensuring compliance. The policies and procedures also set out the consequences of breach. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and that spot security audits will be conducted on a monthly basis. It is the responsibility of the Security Officer to initiate security audits at the prescribed intervals.

18. Log of Security Breaches

Inscyte Corporation maintains a *Log of Security Breaches* as a perpetual archive of *Security Breach Report*s setting out:

- Incident report number (unique for each incident)
- The incident report date
- The name/title of the person(s) who discovered/reported the breach security
- The name/title of the person(s) who investigated the breach of security
- The date/time of the breach (or estimate thereof)
- The evidence that lead to the discovery of the breach of security
- Likelihood and/or evidence that a breach of privacy also occurred (if any)
- Containment procedures (what was done to contain the breach, when and by whom)
- Date of containment
- Suspected perpetrator the breach (if known)
- The motivation/cause for the breach (or suspected motivation/cause)



- Description of security controls that were compromised
- Description of how the security controls were compromised
- Recommendations for changes and mitigating strategies
- The agent(s) responsible for implementing the recommendations
- The date each recommendation is expected to be addressed
- The manner in which each recommendation is expected to be addressed
- Sign-off/approval name, title and date (date investigation was completed)

In the event that a breach of privacy occurs within the context of a breach of security, the *Log of Privacy Breaches* contains additional information such as the nature of the personal health information that was or may have been compromised, the containment measures taken, and the health information custodians or other organizations that were notified about the breach.

Part 3 – Human Resources Documentation

1. Policy and Procedures for Privacy Training and Awareness

Inscyte has developed and implemented a policy requiring its agents to attend initial privacy awareness training upon hiring as well as ongoing privacy awareness training.

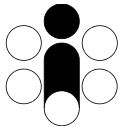
The policy specifies that Privacy Awareness Training shall be provided to agents before an individual is granted access to secured premises or information systems containing personal health information. It is the responsibility of the Privacy Officer to notify agents responsible for administering privacy training about individuals requiring initial privacy training at least three (3) weeks prior to the training session. This notification is to be made by in writing via email or other means.

The policy further requires that privacy awareness training sessions be conducted at least twice per year, but preferably on a quarterly basis in conjunction with Inspirata's quarterly all staff meetings, and that all agents are required to attend these sessions (unless away due to illness or vacation) and that each agent attend at minimum two training sessions each year. Notification of upcoming training meetings is made by email to all staff. In the event that an individual misses three consecutive training sessions, it is the responsibility of the Privacy Officer to notify the individual and schedule a "special" training session at the earliest opportunity.

The policy designates the Privacy Officer as being responsible for ensuring that agents obtain privacy awareness training and for scheduling and preparing quarterly privacy awareness training sessions.

The policy sets out the content of the initial privacy awareness training as follows:

1. Definition of "personal health information".
2. Explanation for the need for privacy regarding health information
3. A description of the Office of the Information and Privacy Commissioner of Ontario
4. Description of the Act, its purpose and the roles of health information custodians, prescribed persons, and prescribed entities.
5. Description of the status of Inscyte Corporation under the Act and the duties and responsibilities that arise as a result of this status.
6. Description of the personal health information held by Inscyte and the health information custodians from whom the information is collected.
7. Explanation of the purposes for which the personal health information is collected.
8. Description of the limitations on the uses of the personal health information.
9. Description of the users of CytoBase.
10. Explanation of how the collection and use is permitted by the Act and its regulation.



11. Description of the status of Inspirata as agent of Inscyte and the privacy governance and accountability framework.
12. Explanation of the privacy program, including the key activities of the program and the persons that have been delegated day-to-day authority to manage the privacy program.
13. Limitations placed on access to and use of the personal health information by Inspirata.
14. An overview of Inscyte's *Privacy Policies and Procedures* that have been implemented and the obligations arising from these policies and procedures.
15. Description of the administrative, technical, and physical safeguards implemented to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.
16. A description of the policies and procedures that must be followed in the event that an agent is requested to disclose personal health information.
17. The duties and responsibilities of all agents in adhering to the administrative, technical and physical safeguards put in place.
18. Discussion of the purpose and content of the standard *Personal Health Information Confidentiality and Non-Disclosure Agreement* that each agent is required to execute.
19. Definition of "breach of privacy"
20. Consequences of a breach of the privacy policies and procedures
21. An overview of the Policy and Procedures for Privacy Breach Management and the duties and responsibilities imposed on agents in identifying, reporting, containing and participating in the investigation and remediation of privacy breaches.

The policy and procedures also require that quarterly privacy training sessions be formalized and standardized and to address the following topics at minimum:

1. Reminder of the status of Inscyte Corporation under the Act and the duties and responsibilities that arise as a result of this status.
2. Reminder of the status of agents of Inscyte and review of the privacy governance and accountability framework.
3. Review of what is and what is not "personal health information"
4. Review of recent breaches of privacy with respect to CytoBase (if any).
5. Review and discussion of recent breaches of privacy in the industry (case studies) as reported through the Office of the Information and Privacy Commissioner, Ontario, or other authorities in Canada or the U.S.
6. Review and discussion of specific policies and procedures applying to specific agent roles.
7. Review and discussion of new or amended policies and procedures since the last training session, if any.
8. Discussion regarding specific privacy policies or procedures arising from questions, or recommendations resulting from privacy audits, privacy impact assessments, threat risk analyses, privacy complaints or privacy breach reports.

9. Discussion regarding any changes to the Act and its regulations or recent orders issued by the Office of the Information and Privacy Commissioner, Ontario that may impact on the privacy program.

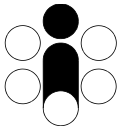
The policy and procedures regarding privacy awareness training require that each individual sign the attendance sheet at each training session (initial, quarterly, or special) and that the attendance sheets be retained in perpetuity in Inscyte's privacy document archives. The policy designates the Privacy officer as being responsible for tracking attendance and maintaining the training attendance log accurate and up to date.

The process of tracking attendance consists of printing an attendance sheet for each training session. The attendance sheet consists of the date of the training session, the type of session (initial, routine quarterly, or special) and, in the case of initial or special training, the names of the designated attendees; otherwise for routine quarterly training sessions a complete list of all agents of Inscyte.

At the conclusion of the training session each attendee is required to sign beside their name on the attendance sheet. After all attendees have signed, the sheet is verified and signed-off by the Privacy Officer or Security Officer. The attendance sheet is then scanned into a computer image file and placed in the privacy document archives. In addition, the cumulative number of sessions attended by each agent since the start of his/her engagement is maintained. Further, the content (slide show & any handouts) of each training session is retained. The policies designate the Privacy Officer as being responsible for maintain this documentation in Inscyte's privacy document archives.

Beyond the requirements of Inscyte's policy and procedures regarding privacy awareness training, Inspirata, as a software engineering firm working in the healthcare domain, with many customers who are health information custodians across Canada and the U.S., promotes a culture of sensitivity to privacy issues on a daily basis by encouraging all staff to be vigilant of hazards and practices that may endanger patient privacy and to report these openly for discussion and remediation. Inspirata communicates this culture of sensitivity by sending email updates with news of recent privacy/security breaches in the healthcare industry and changes to legislation and/or practices as these occur. In addition, privacy matters are discussed at weekly management meetings as part of operations reports.

Inscyte requires its agents to comply with its policies and procedures regarding privacy awareness training and designates the Privacy Officer as being responsible for monitoring and ensuring compliance. The policy and procedures set out the consequences of breach. Inscyte's policy and procedures in respect of privacy audits stipulate that compliance will be audited at minimum on an annual basis and that it is the responsibility of the Privacy Officer to initiate audits at the prescribed intervals.



Inscyte's privacy policies also require its agents to notify Inscyte at the first reasonable opportunity, in accordance with the Policies and Procedures for Privacy Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.

2. Log of Attendance at Initial Privacy Orientation and Ongoing Privacy Training

Inscyte Corporation maintains a log of the attendance of agents at initial privacy awareness training, ongoing quarterly privacy training and special training sessions. The log includes the name of the individual, the date that the individual attended privacy training and the type of training session (initial, quarterly, or special).

3. Policy and Procedures for Security Training and Awareness

Inscyte has developed and implemented a policy requiring its agents to attend initial security awareness training upon hiring as well as ongoing security awareness training. In practice, privacy awareness and security awareness training are combined into concurrent sessions.

The policy specifies that security awareness training shall be provided to agents before the individual completes his/her three-month probationary period and before the individual is granted access to secured premises or information systems containing personal health information. The policy further requires that security awareness training sessions be held at least twice per year, but preferably on a quarterly basis in conjunction with Inspirata's quarterly all staff meetings, and that all agents are required to attend these sessions (unless away due to illness or vacation) and that each agent attend at minimum two training sessions each year. In the event that an agent misses three consecutive training sessions, it is the responsibility of the Privacy Officer to notify the individual and schedule a "special" training session at the earliest opportunity.

The policy designates the Privacy Officer as being responsible for ensuring that agents obtain security awareness training and for scheduling and preparing quarterly security awareness training sessions, which are combined in practice with privacy awareness training as described in the section above.

The policy sets out the content of the initial security awareness training as follows:

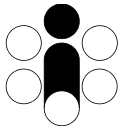
1. An overview of Inscyte's *Security Policies and Procedures* that have been implemented and the obligations arising from these policies and procedures.
2. An explanation of the security program, including the key activities of the program and the persons that have been delegated day-to-day authority to manage the security program.

3. Description of the security governance and accountability framework.
4. The administrative, technical, and physical safeguards implemented to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.
5. The duties and responsibilities of agents in implementing the administrative, technical and physical safeguards put in place.
6. A definition of "breach of security" and its relationship to a breach of privacy.
7. The consequences of breach of the security policies and procedures.
8. An overview of the Policy and Procedures for Security Breach Management and the duties and responsibilities imposed on agents in identifying, reporting, containing, and participating in the investigation and remediation of security breaches.

The policy and procedures also require that quarterly security training sessions be formalized and standardized and address the following topics at minimum:

1. Review of the security governance and accountability framework.
2. Review of the nature of physical and technical security controls implemented.
3. Discussion of continued adequacy of security controls with regard to emerging technologies and best practices.
4. Review of recent breaches of security with respect to CytoBase (if any).
5. Review and discussion of recent breaches of security in the industry (case studies) as reported through the Office of the Information and Privacy Commissioner, Ontario, or other authorities in Canada or the U.S.
6. Discussion regarding specific security policies or procedures arising from questions, or recommendations resulting from privacy impact assessments, security audits, threat risk analyses, security complaints or security breach reports.
7. Discussion regarding any changes to the Act and its regulations or recent orders issued by the Office of the Information and Privacy Commissioner, Ontario that may impact on the security program.
8. Review and discussion of specific policies and procedures applying to specific agent roles.
9. Review and discussion of new or amended policies and procedures since the last training session, if any.

The policy and procedures regarding security awareness training require that each individual sign the attendance sheet at each training session (initial, quarterly, or special) and that the attendance sheets be retained in perpetuity in Inscyte's privacy document archives. The policy designates the Privacy officer as being responsible for tracking attendance and maintaining the training attendance log accurate and up to date.



The process of tracking attendance consists of printing an attendance sheet for each training session. The attendance sheet consists of the date of the training session, the type of session (initial, routine quarterly, or special) and, in the case of initial or special training, the names of the designated attendees; otherwise for routine quarterly training sessions a complete list of all agents of Inscyte.

At the conclusion of the training session each attendee is required to sign beside their name on the attendance sheet. After attendees have signed, the sheet is verified and sign-off by the Privacy Officer or Security Officer. The attendance sheet is then scanned into a computer image file and placed in the privacy document archives. In addition, the cumulative number of sessions attended by each agent since the start of his/her engagement is maintained. Further, the content (slide show & any handouts) of each training session is retained. The policies designate the Privacy Officer as being responsible for maintain this documentation in Inscyte's privacy document archives.

Beyond the requirements of Inscyte's policy and procedures regarding security awareness training, Inspirata, as a software engineering firm working in the healthcare domain, with many customers who are health information custodians across Canada and the U.S., promotes a culture of sensitivity to security issues on a daily basis by encouraging all staff to be vigilant of hazards and practices that may place secured assets at risk and to report these openly for discussion and remediation. Inspirata communicates this culture of sensitivity by sending email updates with news of recent privacy/security breaches in the healthcare industry and changes to legislation and/or practices as these occur. In addition, privacy matters are discussed at weekly management meetings as part of operations reports.

Inscyte requires its agents to comply with its policies and procedures regarding security awareness training and designates the Privacy Officer as being responsible for monitoring and ensuring compliance. The policy and procedures set out the consequences of breach. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and through random spot checks, and that it is the responsibility of the Security Officer to initiate security audits at the prescribed intervals.

Inscyte's privacy policies require agents of Inscyte to notify Inscyte at the first reasonable opportunity, in accordance with the Policies and Procedures for Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.

4. Log of Attendance at Initial Security Orientation and Ongoing Security Training

Inscyte Corporation maintains a log of the attendance of agents at initial security awareness training, ongoing quarterly security training and special training sessions. The log includes the

name of the individual, the date that the individual attended security training and the type of training session (initial, quarterly, or special).

5. Policy and Procedures for the Execution of Confidentiality Agreements by Agents

Inscyte's policy states that its agents shall be required to execute a signed and witnessed *Personal Health Information Confidentiality and Non-Disclosure Agreement* in accordance with the minimum content standard of the template confidentiality agreement.

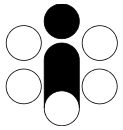
The policy further requires that *Personal Health Information Confidentiality and Non-Disclosure Agreements* are to be executed before the start of employment or contract, prior to giving the individual access, if any, to personal health information, and that the agreements survive the duration of employment or contract.

The policy states that it is the responsibility of the Privacy Officer to ensure that all agents of Inscyte who may reasonably be expected to work with personal health information have a signed and witnessed *Personal Health Information Confidentiality and Non-Disclosure Agreement* in effect. The confidentiality agreements are a mandatory condition of employment or contract and must be executed before commencement of work.

The policy does not require *Personal Health Information Confidentiality and Non-Disclosure Agreements* to be re-executed on an annual basis but states that, should the standard template agreement be amended, all current agents shall be required to re-execute the new amended agreement.

The process of obtaining signed and witnessed *Personal Health Information Confidentiality and Non-Disclosure Agreements* consists of presenting each agent with an engagement package that includes the pre-printed standard confidentiality agreement. The individual is given time to read and understand the agreement. Any questions or concerns are addressed, including an explanation of the privacy and security program as required. The individual must execute the agreement as a condition of engagement. After the individual signs the agreement it must be dated and witnessed. One copy of the agreement is given to the individual and another copy is retained in the privacy document archives.

The policy and procedures also require a log of executed *Personal Health Information Confidentiality and Non-Disclosure Agreements* to be maintained and designate the Privacy Officer as being responsible for maintaining this log. The policies require that documentation related to the execution of confidentiality agreements be retained in Inscyte's privacy document archives and designate the Privacy Officer as being responsible for ensuring the documents are retained.



Inscyte requires its agents to comply with its policies and procedures regarding execution of confidentiality agreements and designates the Privacy Officer as being responsible for monitoring and ensuring compliance. The policy and procedures set out the consequences of breach. Inscyte's policy and procedures in respect of privacy audits stipulate that compliance will be audited at minimum on an annual basis and that it is the responsibility of the Privacy Officer to initiate privacy audits at the prescribed intervals.

Inscyte's security policies require agents of Inscyte to notify Inscyte at the first reasonable opportunity, in accordance with the Policies and Procedures for Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.

6. Template Confidentiality Agreement with Agents

Inscyte's policy states that its agents who may reasonably be expected to work with personal health information to execute a signed and witnessed *Personal Health Information Confidentiality and Non-Disclosure Agreement* (the agreement) addressing Inscyte's minimum content standard as set out below.

General Provisions

The agreement provides a definition of personal health information in accordance with the Act and its regulations.

The agreement identifies Inscyte Corporation as a prescribed person under the Act and describes the duties and responsibilities arising from this status.

The agreement states that the individuals executing the agreement are agents of Inscyte in respect of personal health information and describes the duties and responsibilities associated with this status.

The agreement requires agents to comply with the provisions of the Act and its regulation relating to prescribed persons or prescribed entities, as the case may be, and with the terms of the agreement as may be amended from time to time.

The agreement requires the agent to acknowledge that he/she has read, understood and agrees to comply with the Inscyte's Privacy & Security Policies and Procedures as implemented and as may be amended from time to time following the execution of the agreement.

Obligations with Respect to Collection, Use and Disclosure of Personal Health Information

The agreement stipulates that any and all collection, use, disclosure, transfer and/or disposal of personal health information by agents on behalf of Inscyte shall be in compliance with Inscyte's *Privacy Code* and its *Privacy & Security Policies and Procedures* and the limitations, conditions and/or restrictions imposed therein.

The agreement prohibits agents from collecting, using or disclosing personal health information if other information will serve the purpose and from collecting, using or disclosing more personal health information than is reasonably necessary to meet the purpose.

Termination of the Contractual, Employment or Other Relationship

In accordance with policies for actions to be taken at the termination of employment, contract, or other relationship, the agreement requires agents to surrender any and all records of personal health information in their possession, in printed format or on portable media, prior to termination, and to return all identification cards, access cards and/or keys, on or before the date of termination. The agreement further permits inspection of an agent's place(s) of work and any personal mobile devices to ensure that no personal health information remains in the individual's possession.

Notification

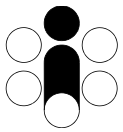
The agreement requires the agent to notify the Privacy Officer at the first reasonable opportunity if the agent breaches or believes that there may have been a breach of the agreement or if the agent breaches or believes that there may have been a breach of Inscyte's Privacy & Security Policies and Procedures.

Consequences of Breach and Monitoring Compliance

The agreement states that compliance with the agreement and the Privacy & Security Policies and Procedures is monitored and audited by the Privacy Officer and Security Officer and that a breach of the agreement, a breach of privacy or a breach of security may result in the termination of employment or contract. The agreement also stipulates that unauthorized disclosure or inappropriate use of personal health information may also result in legal action taken by affected parties against the agent.

7. Log of Executed Confidentiality Agreements with Agents

Inscyte Corporation policies and procedures require maintaining a log of confidentiality agreements that have been executed by agents of Inscyte. The log includes the name of the individual, the date of commencement of employment or contract, and the dates that *Personal Health Information Confidentiality and Non-Disclosure Agreements* were executed by each individual.



8. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program

Inscyte's privacy policy designates the position of "Privacy Officer" as having day-to-day authority to manage the privacy program. The Privacy Officer of Inscyte's agent Inspirata is the acting Privacy Officer of Inscyte Corporation.

The job description specifies that the Privacy Officer of Inscyte reports to the President of Inscyte. The job description specifies that Privacy Officer is responsible for the following:

- Developing, implementing, reviewing and amending privacy policies, procedures and practices.
- Ensuring compliance with the privacy policies, procedures and practices implemented.
- Ensuring transparency of the privacy policies, procedures and practices implemented.
- Facilitating compliance with the Act and its regulation.
- Ensuring agents are aware of the Act and its regulation and their duties thereunder.
- Ensuring agents are aware of the privacy policies, procedures and practices implemented by Inscyte Corporation and are appropriately informed of their duties and obligations thereunder.
- Directing, delivering, or ensuring the delivery of the initial privacy orientation and the ongoing privacy training and fostering a culture of privacy.
- Conducting, reviewing, and approving privacy impact assessments.
- Receiving, documenting, tracking, investigating, remediating, and responding to privacy complaints pursuant to the Policy and Procedures for Privacy Complaints.
- Receiving and responding to privacy inquiries pursuant to the Policy and Procedures for Privacy Inquiries.
- Receiving, documenting, tracking, investigating and remediating privacy breaches or suspected privacy breaches pursuant to the Policy and Procedures for Privacy Breach Management; and
- Conducting privacy audits pursuant to the Policy and Procedures in Respect of Privacy Audits.
- Monitoring privacy industry standards and developments, including orders and recommendations of the Office of the Information and Privacy Commissioner, Ontario, and bringing forth recommendations to ensure Inscyte's privacy program keeps pace with evolving best practices.

9. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program

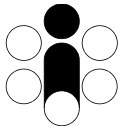
Inscyte's privacy policy designates the position of "Security Officer" as having day-to-day authority to manage the security program. The Security Officer of Inscyte's agent Inspirata is the acting Security Officer of Inscyte Corporation.

The job description specifies that the Security Officer of Inscyte reports to the President of Inscyte. The job description specifies that Security Officer is responsible for the following:

- Developing, implementing, reviewing and amending security policies, procedures and practices.
- Ensuring compliance with the security policies, procedures and practices implemented.
- Ensuring agents are aware of the security policies, procedures and practices implemented by Inscyte Corporation and are appropriately informed of their duties and obligations thereunder.
- Directing, delivering, or ensuring the delivery of the initial security orientation and the ongoing security training and fostering a culture of information security awareness.
- Receiving, documenting, tracking, investigating and remediating information security breaches or suspected information security breaches pursuant to the Policy and Procedures for Information Security Breach Management; and
- Conducting security audits pursuant to the Policy and Procedures in Respect of Security Audits.
- Monitoring industry standards and best practices with respect to technical, physical and environmental security controls, orders and recommendations of the Office of the Information and Privacy Commissioner, Ontario, and bringing forth recommendations to ensure Inscyte's security program keeps pace with evolving technology and best practices.

10. Policy and Procedures for Termination or Cessation of Employment or Contractual Relationship

Inscyte's policies and procedures require its agents to notify Inscyte of the termination of employment, contract, or other relationship. The policy requires that the Privacy Officer be notified in writing identifying the agent who ceased to be employed or contracted, the date of the termination, and acknowledgment that the individual has surrendered all personal health information in his/her possession, on portable media or on paper, that the individual's personal mobile devices (if any) do not contain any personal health information, that the individual has returned all identification cards, access cards and/or keys, and that the individual has been advised that the terms and conditions of his/her *Personal Health Information Confidentiality and Non-Disclosure Agreement r*emain in force following termination. Inscyte's policies specify that such notification will be provided within ten (10) business days following the termination. In the



event that the termination concerns an agent who had been granted access to personal health information in CytoBase, the policies require that the President of Inscyte be notified in the same manner and designate the Privacy Officer are being responsible to provide this notification.

The policies require the following actions to be taken upon cessation of employment, contract, or other relationship to supervise and ensure that all personal health information, identification cards, access cards and/or keys are surrendered and returned, and that all information system access accounts are deactivated:

(a) Obtain all access cards issued to the individual.
(b) De-activate the individual's access cards.
(c) De-activate the individual's computer network access account(s).
(d) De-activate the individual's application access account(s).
(e) Check the individual's computer workstation(s) and mobile devices (if any) for the presence of personal health information.
(f) Archive or destroy any PHI found on the individual's computer(s) or mobile devices.
(g) Check the individual's physical workspace for any portable media or printed information that may contain personal health information and either archive these in a secure location or dispose of (destroy) the personal health information.
(h) Provide the individual with written notice that the provisions of the confidentiality and non-disclosure agreement agreed to by the individual as a condition of employment or contract remain in force.

The policy designates the Security Officer as being responsible for ensuring the above actions are carried out and as the agent to whom personal health on portable media or paper records, identification cards, access cards and/or keys should be returned. Access cards and any other assets that could affect privacy or security that are not returned are remotely de-activated.

The policy further requires that upon termination all related privacy and security documentation, such as the *Log of Individuals Having Access to Premises*, the *Log of Accounts Having Access to PHI*, and the *Log of Authorized Personnel* who have been granted access to CytoBase information, to be updated to reflect the termination and de-activation of access rights. The policies specify that it is the responsibility of the Security Officer to ensure that the documentation is updated within ten (10) business days following the termination and to advise the Privacy Officer of same so that notification can be forwarded to the President of Inscyte.

Inscyte Corporation requires its agents to comply with its policy and procedures regarding cessation of employment or contractual relationships and designates the Privacy Officer as being responsible for monitoring and ensuring compliance. The policies and procedures set out the consequences of breach. Inscyte's policy and procedures in respect of privacy audits stipulate that compliance will be audited at minimum on an annual basis and that it is the responsibility of

the Privacy Officer to initiate privacy audits at the prescribed intervals. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and through random spot checks, and that it is the responsibility of the Security Officer to initiate security audits at the prescribed intervals.

Inscyte's policies and procedures require its agents to notify Inscyte at the first reasonable opportunity, in accordance with the Policy and Procedures for Privacy Breach Management and/or the Policy and Procedures for Information Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.

11. Policy and Procedures for Discipline and Corrective Action

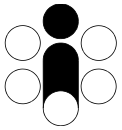
Inscyte's policy for discipline and corrective action in respect of personal health information requires its agents to take corrective actions in accordance with its policies and procedures to remedy non-compliance with Privacy & Security Policies and Procedures.

The policy states that in the event of an incident of non-compliance, it is the responsibility of the Privacy Officer to investigate the incident by:

1. Interviewing the individual(s) involved to ascertain the circumstances and reasons surrounding the non-compliance. In particular, to determine whether the non-compliance was intentional or accidental and whether or not the individual(s) had been aware of the policies and procedures that were breached.
2. Assessing the severity and consequences of the non-compliance. In particular, determining if the non-compliance had or could have resulted in an unauthorized disclosure or use of personal health information.
3. Assessing if the incident is an individual(s) first incident of non-compliance or a repeat incident.

The policy provides general guidelines for corrective actions depending on the results of the investigation as follows:

a) If the non-compliance is a first incident, is accidental or due to a lack of awareness of policies and procedures, and unauthorized disclosure or use of personal health information did not occur, then a warning to the individual(s) and review of applicable policies and procedures is sufficient. It is the responsibility of the Privacy Officer to deliver the warning either verbally or by email and to ensure the individuals involved understand the importance of adhering to the policies and procedures and the consequences of failing to do so.



b) If the non-compliance is a repeat incident, is accidental or due to a lack of awareness of policies and procedures, then a written warning letter to the individual(s) describing the incident, the policies and procedures that were breached, and a warning that further non-compliance may result in disciplinary action is to be prepared for each individual involved. It is the responsibility of the Privacy Officer to prepare the letter, serve the letter to the individual(s) and notify the President of Inscyte that such a warning was served. The policies require a copy of the letter to be retained in the privacy document archives.

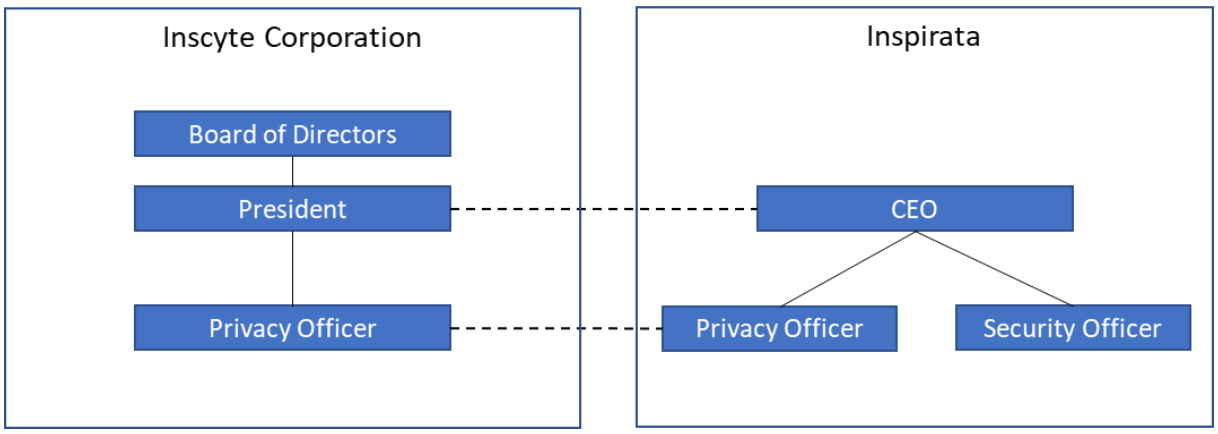
c) If the non-compliance was determined to be intentional, or a repeat incident following a previous written warning letter, or has resulted in the unauthorized disclosure or use of personal health information, the matter is to be immediately referred to the President of Inscyte and to agents of Inscyte for determination of appropriate disciplinary actions, which may include termination of employment, contract or other relationship.

Part 4 – Organizational and Other Documentation

1. Privacy Governance and Accountability Framework

Inscyte Corporation's Privacy and Security Program is implemented and managed by its agent Inspirata, under contract to Inscyte Corporation for the day-to-day operations of CytoBase. Inspirata is responsible for ensuring compliance with the Act and its regulation in this regard and for implementing and ensuring compliance with Inscyte's privacy policies and procedures.

The privacy governance and accountability framework is depicted in the diagram below.

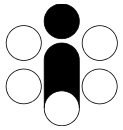


The privacy governance and accountability framework stipulates that the President of Inscyte Corporation is ultimately accountable for ensuring that Inscyte and its agents comply with the Act and its regulation and comply with its Privacy Code and its Privacy Policies and Procedures. The President of Inscyte is accountable to the Board of Directors of Inscyte Corporation, which is comprised of representatives from the member laboratories (health information custodians) that provide personal health information to CytoBase.

The Privacy Officer of Inscyte's agent Inspirata has been delegated day-to-day authority to manage the privacy program and as such is the acting Privacy Officer of Inscyte. The Privacy Officer reports directly to the CEO of Inspirata. The CEO of Inspirata is accountable to the President of Inscyte Corporation in regards to fulfilling Inspirata's obligations with respect to implementing and managing Inscyte's privacy program.

The Privacy Officer is supported by Inspirata's Vice-President of Engineering and Operations Manager, who are authorized to delegate work to software development, quality assurance, technical support, and human resource departments.

The role of Inscyte's Board of Directors in respect of the privacy program is to review and approve of changes brought before the Board by the President of Inscyte. The Board may also request an



update on the privacy program from the President on a regular or ad hoc basis, but at the minimum, the Board is updated on an annual basis. The update addresses the initiatives undertaken by the privacy program including privacy training and the development and implementation of privacy policies, procedures, and practices. It also includes a discussion of privacy audits and privacy impact assessments conducted, including the results of and recommendations arising from the privacy audits and privacy impact assessments and the status of implementation of the recommendations. The Board of Directors is also advised of any privacy breaches and privacy complaints which were investigated, including the results of and any recommendations arising from these investigations and the status of implementation of the recommendations. The privacy program is not currently overseen by a committee of the Board of Directors.

The privacy governance and accountability framework is documented in Inscyte's privacy document archives and is communicated to agents of Inscyte by the Privacy Officer as part of initial privacy training and on-going privacy awareness training.

2. Security Governance and Accountability Framework

Inscyte Corporation's Privacy and Security Program is implemented and managed by its agent Inspirata, under contract to Inscyte Corporation for the day-to-day operations of CytoBase. Inspirata is responsible for ensuring compliance with the Act and its regulation in this regard and for implementing and ensuring compliance with Inscyte's security policies and procedures.

The security governance and accountability framework stipulates that the President of Inscyte Corporation is ultimately accountable for ensuring that Inscyte and its agents comply with the Act and its regulation and comply with its Security Policies and Procedures. The President of Inscyte is accountable to the Board of Directors of Inscyte Corporation, which is comprised of representatives from the member laboratories (health information custodians) that provide personal health information to CytoBase.

The Security Officer of Inscyte's agent Inspirata has been delegated day-to-day authority to manage the security program and as such is the acting Security Officer of Inscyte. The Security Officer reports directly to the CEO of Inspirata. The CEO of Inspirata is accountable to the President of Inscyte Corporation regarding fulfilling Inspirata's obligations with respect to implementing and managing Inscyte's security program.

The Security Officer is supported by Inspirata's Vice-President of Engineering and its Operations Manager, who are authorized to delegate work to software development, quality assurance, technical support, and human resource departments.

The role of Inscyte's Board of Directors in respect of the security program is to review and approve of changes brought before the Board by the President of Inscyte. The Board may also request an update on the security program from the President on a regular or ad hoc basis, but at the minimum, the Board is updated on an annual basis. The update addresses the initiatives

undertaken by the security program including security training and the development and implementation of security policies, procedures, and practices. It also includes a discussion of security audits and vulnerability assessments conducted, including the results of and recommendations arising from the privacy audits and privacy impact assessments and the status of implementation of the recommendations. The Board of Directors is also advised of any security breaches and security complaints which were investigated, including the results of any recommendations arising from these investigations and the status of implementation of the recommendations. The security program is not currently overseen by a committee of the Board of Directors.

The security governance and accountability framework is documented in Inscyte's privacy document archives and is communicated to agents of Inscyte by the Security Officer as part of initial security training and on-going security training.

3. Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program

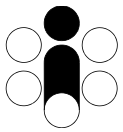
Inscyte does not currently have committees overseeing or having roles in the privacy or security program. In the event that such committees should be convened in the future, Inscyte shall ensure that appropriate terms of reference shall be specified for these committees identifying the membership of the committee, the chair of the committee, the mandate and responsibilities of the committee in respect of the privacy and/or the security program and the frequency with which the committee meets. The terms of reference shall also set out to whom the committee reports; the types of reports produced by the committee, if any; the format of the reports; to whom these reports are presented; and the frequency of these reports.

4. Corporate Risk Management Framework

Inscyte Corporation's policy requires that its agent Inspirata implement a risk management framework to identify, assess, mitigate and monitor risks, including risks that may negatively affect Inscyte's ability to protect the privacy of individuals whose personal health information is received, to maintain the confidentiality of that information, and to maintain the availability of the information.

Inscyte's policy requires its agent Inspirata to have processes in place to identify and manage risks with respect to the safeguarding of personal health information and its availability; to ensure that identified risks are communicated to the Privacy Officer and Security Officer; and to ensure that risks are recorded in a *Corporate Risk Register*, and acted upon to monitor, mitigate or obviate risks in a timely manner.

Inscyte's policies state that it is the responsibility of every agent to be vigilant of and identify circumstances that may put patient privacy and/or the safeguarding of personal health information or its availability at risk. The policies require that each identified risk is to be reported



as soon as possible to the Privacy Officer, either verbally or by email. The policies specify that it is the responsibility of the Privacy Officer to ensure that each reported risk is recorded in the *Corporate Risk Register* and that each risk is quantified in terms of the likelihood of occurrence and severity of impact (consequence) should the risk materialize. The combination of likelihood and severity are used to compute an overall threat ranking for each risk.

The risk management policy requires review of *the Corporate Risk Register* at minimum on a quarterly basis and requires acting on risks in order of ranking (from highest to lowest) for risks exceeding a specified threat rank threshold. It is the responsibility of the Privacy Officer to ensure that the *Corporate Risk Register* is reviewed and to track and ensure that risks are monitored and mitigated in accordance with this policy.

Acting on risks involves a review of each risk by Inspirata's Vice-President of Engineering and Inspirata's Operations Manager to formulate recommendations and strategies to mitigate or obviate an identified risk. This may include recommendations to engage third-party service providers and/or outside experts. Recommendations for mitigating risks that will incur substantial expense to implement require the prior approval of the CEO of Inspirata and may be subject to Inscyte's policy and procedures in respect of change management.

It is the responsibility of the Privacy Officer to ensure that recommendations are recorded in the *Corporate Risk Register* including the names of agent(s) responsible for implementing the recommendations and the target date for the implementation.

The policy states that when mitigating strategies/changes are implemented, the *Corporate Risk Register* is to be updated to include a description of the mitigating strategy/change, the date of completion, and a re-assessment of the risk ranking.

5. Corporate Risk Register

Inscyte Corporation requires its agent Inspirata to maintain an on-going and perpetual *Corporate Risk Register* that records and identifies each risk identified that may negatively affect the ability of Inscyte to protect the privacy of individuals whose personal health information is received, to maintain the confidentiality of that information, and to ensure the availability of the information to authorized parties. The minimum content of the *Corporate Risk Register* is as follows:

(a) Risk number (unique to each risk)
(b) Date of entry
(c) Name of person making the entry
(d) Description of the risk
(e) The likelihood of occurrence
(f) The impact of occurrence
(g) Threat rank (original)

(h) Risk status
(i) Recommendations for monitoring and/or mitigating the risk
(j) The agent(s) responsible for implementing the recommendations
(k) The target date for implementing the recommendations
(l) The date the recommendations were implemented/completed
(m) Threat rank after mitigation

6. Policy and Procedures for Maintaining a Consolidated Log of Recommendations

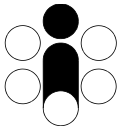
Inscyte Corporation policy requires its agent Inspirata to maintain a centralized, on-going and perpetual *Consolidated Log of Recommendations* of all recommendations arising from privacy impact assessments, threat risk assessments, privacy audits, security audits and the investigation of privacy breaches, privacy complaints and security breaches. The policy states that the *Consolidated Log of Recommendations* shall also include recommendations made by the Information and Privacy Commissioner of Ontario that must be addressed by Inscyte Corporation prior to the next review of its practices and procedures.

The policy stipulates that it is the responsibility of the Privacy Officer to ensure that the *Consolidated Log of Recommendations* is maintained accurate, complete, and up-to-date and that the log shall be updated as required when any of the following events occur:

(a) A Privacy Impact Assessment (PIA) is conducted
(b) A Threat Risk Analysis (TRA) is conducted
(c) The Corporate Risk Register is updated
(d) A privacy/security audit is conducted
(e) A privacy/security breach is documented
(f) A privacy complaint is resolved
(g) A review by the Information and Privacy Commissioner, Ontario is conducted
(h) A logged recommendation has been addressed

The policy further states that the *Consolidated Log of Recommendations* be reviewed at minimum on a quarterly basis to ensure that the recommendations are addressed in a timely manner and designates the Privacy Officer as being responsible to initiate a review of the log.

Inscyte Corporation requires its agents to comply with its policy and procedures regarding maintaining and acting upon the *Consolidated Log of Recommendations* and designates the Privacy Officer as being responsible for monitoring and ensuring compliance. The policy and procedures set out the consequence of breach. Inscyte's policy and procedures in respect of privacy audits stipulate that compliance will be audited at minimum on an annual basis and that



it is the responsibility of the Privacy Officer to initiate privacy audits at the prescribed intervals. Inscyte's policy and procedures in respect of security audits stipulate that compliance will be audited at minimum on an annual basis and through random spot checks, and that it is the responsibility of the Security Officer to initiate security audits at the prescribed intervals.

Inscyte's policies and procedures require its agents to notify Inscyte at the first reasonable opportunity, in accordance with the Policy and Procedures for Privacy Breach Management and/or the Policy and Procedures for Information Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.

7. Consolidated Log of Recommendations

Inscyte Corporation's policy requires its agent Inspirata to maintain an on-going and perpetual *Consolidated Log of Recommendations* of all recommendations arising from privacy impact assessments, threat risk assessments, privacy audits, security audits, the investigation of privacy breaches, the investigation of privacy complaints, the investigation of information security breaches and reviews by the Information and Privacy Commissioner of Ontario. The policy requires the log to contain the following information at minimum:

(a) Recommendation number (unique to each recommendation)
(b) Date of entry
(c) The name of the person making the entry
(d) Recommendation status
(e) Type of action giving rise to the recommendation (e.g. audit, breach, TRA etc.)
(f) Date of the action giving rise to the recommendation
(g) References to supporting documents
(h) Summary of the recommendation
(i) The actions to be taken to address the recommendation
(j) The agents responsible for carrying out these actions
(k) The target date these actions are to be completed
(l) The actual date the actions were completed

8. Business Continuity and Disaster Recovery Plan

Inscyte Corporation's policy requires that its agent Inspirata develop and implement policies and procedures to protect and ensure the continued availability of CytoBase in the event of short and long-term business interruptions, and in the event of threats to the operating capabilities of CytoBase arising from natural, human, environmental and technical disruptions. Since CytoBase is hosted, operated and maintained by Inspirata within its computing environment, it is covered by Inspirata's business continuity and disaster recovery plan.

Inspirata's policies and procedures in respect of operating and maintaining its datacenter specify the measures required to detect and warn against threats, outages, or potential outages, arising

from power failures, equipment failures, environmental threats (fire, water or excessive heat), network intrusions and physical break-ins. It is the responsibility of Inspirata's Operations Manager to ensure that such alarms and warning systems are in place and functional at all times except for scheduled maintenance.

Inspirata's policies require specific personnel to be contacted, by telephone, at the first available opportunity, whenever an alarm or warning system is activated. To this end, Inspirata maintains hierarchical lists of Inspirata personnel to be contacted for each type of alarm or warning system and designates the Operations Manager as being responsible for maintaining these lists accurate and up to date.

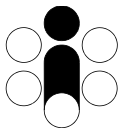
Upon warning or discovery of a threat, outage, or a potential outage, the policy states that it is the responsibility of Inspirata's Operations Manager to assess the extent and severity of the incident and to notify the CEO, Privacy Officer and Security Officer of Inspirata about the incident at the first available opportunity either verbally or by email. The policy specifies that the criteria for assessing the severity of a threat or outage must include estimating the likelihood that an interruption to normal operations will occur, the duration of such an interruption, the potential for loss/damage to assets or security controls, and the potential for a security or privacy breach occurring as a result of the threat or outage.

The policies further require an assessment to be made to determine if a breach of privacy has occurred, or is likely to occur, as a result of the threat, outage, or a potential outage. The policies set out the assets to be examined in making this determination and designate the Operations Manager as being responsible for inspecting the assets and reporting the findings to the Privacy Officer for a final determination. In the event that a breach of privacy has, or is suspected to have occurred, then the policy requires that Inscyte Corporation's procedures in respect of Privacy Breach Management shall also take effect.

The policies also require that an assessment be made to determine if a breach of security has occurred in relation to the threat or outage. The policies set out the assets to be examined in making this determination and designate the Operations Manager as being responsible for inspecting the assets and reporting the findings to the Security Officer for a final determination. In the event that a breach of security has, or is suspected to have occurred, then the policy requires that Inscyte Corporation's procedures in respect of Security Breach Management shall also take effect.

In the event that an unplanned outage occurs, Inspirata's policy requires the Manager of Operations to investigate the outage in detail and prepare a written *Outage Report* containing:

a) The date of the outage
b) Description of the outage



c) Identification of affected assets
d) Indication if a breach of privacy or security has occurred
e) Assessment of the cause of the outage
f) Recommended actions to restore operations
g) Estimated time and cost to restore operations
h) The agent(s) responsible for carrying out the actions to restore operations

Inspirata's policies require that this report be provided to the CEO and Vice-President of Engineering of Inspirata as soon as possible following an outage, and that in the event that the costs of repairs shall exceed a prescribed threshold, the CEO of Inspirata is required to provide approval to proceed.

In respect of CytoBase, the business continuity and disaster recovery plan requires that the President of Inscyte and all affected stakeholders of Inscyte shall be notified of an outage in the event that the estimated time to remedy the outage and restore operations exceeds or is likely to exceed twelve (12) hours. In this case, it is the responsibility of the Operations Manager of Inspirata to ensure that notification is sent via email to designated contacts of each stakeholder describing the outage, actions being taken to remedy the outage and the estimated date (and time if applicable) of restoration. In support of this requirement Inspirata maintains a list of stakeholders and contact information. It is the responsibility of the Operations Manager to ensure that this list is maintained accurate and up to date.

Inspirata's business continuity and disaster recovery plan designates Inspirata's Operations Manager as being responsible for conducting an impact assessment of an interruption or threat, including its impact on the technical and physical infrastructure and the operational processes of CytoBase. The plan requires the impact assessment to take into consideration the duration of an interruption, the potential for loss/damage to assets or security controls, and the potential for a security or privacy breach occurring. The plan prescribes that the Operations Manager may engage Inspirata's engineering and technical resources and/or third-party service providers or vendors as may be required to complete the impact assessment. The plan requires the Operations Manager to report the results of the impact assessment in writing to the CEO of Inspirata.

Inspirata's business continuity and disaster recovery plan designates Inspirata's Operations Manager as being responsible for conducting and preparing a detailed damage assessment in order to evaluate the extent of the damage caused by a threat or interruption and the expected effort required to resume, recover and restore infrastructure elements, information systems and/or services related to CytoBase. The plan requires the damage assessment to take into consideration all assets affected by the interruption or threat. The plan prescribes that the Operations Manager may engage Inspirata's engineering and technical resources and/or third-party service providers or vendors as may be required to complete the damage assessment. The

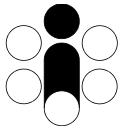
plan requires the Operations Manager to report the results of the damage assessment in writing to the CEO and the Vice-President of Engineering of Inspirata.

Inscyte Corporation designates Inspirata as being responsible for recovery from a threat or outage of CytoBase. Inspirata's business continuity and disaster recovery plan designates Inspirata's Operations Manager as being responsible for taking all appropriate actions to recover from a threat or outage and resume normal operations of CytoBase. The plan includes the priority in which business functions should be restored, instructions and procedures for recovery of each hardware and software asset, and the order in which these assets must be restored in accordance with asset dependencies. The plan prescribes that the Operations Manager may engage Inspirata's engineering and technical resources and/or third-party service providers or vendors as may be required to complete the recovery. The plan requires that the Operations Manager submit a recovery plan to the CEO of Inspirata for approval before taking actions to recover from a threat or outage. Inscyte Corporation is not required to provide prior approval for actions taken by Inspirata to restore normal operations of CytoBase following a threat or outage unless such actions qualify as a change requiring Inscyte's prior approval in accordance with Inscyte's Policy and Procedures in respect of Change Management.

In support of actions to be taken to recover from a threat or outage Inspirata maintains comprehensive and detailed *Asset Inventory and Configuration Documentation* that includes all critical applications and business functions, hardware and software components, software licenses, vendor information, recovery media, ancillary equipment, system network diagrams, hardware configurations, software configurations, configuration settings for database systems and network settings for firewalls, routers, domain name servers, email servers and the like.

Inspirata's policies in respect of business continuity and disaster recovery designate the Operations Manager as being responsible for developing and maintaining the *Asset Inventory and Configuration Documentation* complete and up to date. The policy defines "critical assets" to mean without limitation software applications, supporting software, hardware, ancillary equipment, data holdings, and all third-party services that are required to enable or support Inspirata's core business functions and those of its customers.

Inspirata's business continuity and disaster recovery plan also addresses the testing, maintenance and assessment of the business continuity and disaster recovery measures. Inscyte does not have a policy stipulating a specific frequency at which the disaster recovery plan is to be tested. However, Inscyte requires that a backup and restore procedure is to be carried out to verify disaster recovery on a component level each time a significant hardware and/or software change is made to the CytoBase computing infrastructure. Inspirata validates the restoration procedures and asset configuration information whenever it performs a component upgrade within its computing infrastructure. This occurs on a regular basis as servers are upgraded or replaced, databases are migrated to newer versions, or other equipment, such as firewalls and



routers are replaced and updated. It is the responsibility of the Operations Manager of Inspirata to ensure that tests of the disaster recovery plan, in whole or in part, are performed at the earliest opportunity whenever the computing infrastructure is significantly changed. If disaster recovery tests fail, the Operations Manager is required to ensure that all necessary amendments are made to the disaster recovery plan and its supporting documentation to resolve the deficiency. It is the responsibility of Inspirata's Operations Manager to approve Inspirata's business continuity and disaster recovery plan and any amendments thereto.

It is the responsibility of the Operations Manager of Inspirata to document and publish the most recent edition of Inspirata's Business Continuity and Disaster Recovery Plan in electronic format on Inspirata's business network (for internal use) and on portable media to be retained off-site. Inspirata's policy states that its Business Continuity and Disaster Recovery Plan will be made available to customers of Inspirata that are impacted by the plan, upon written request and prior approval by the CEO of Inspirata.

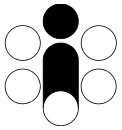
Privacy, Security and Other Indicators

Part 1 – Privacy Indicators

<table>
<tr><th>Categories</th><th>Privacy Indicators</th></tr>
<tr><td>General Privacy Policies, Procedures and Practices</td><td>
Inscyte Corporation has a consolidated set of policies and procedures that apply to Inscyte Corporation, and by extension, Inspirata. since Inspirata acts as Agent for Inscyte in respect to CytoBase.

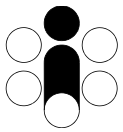
The “Privacy & Security Policies and Procedures Manual” addresses the requirements in Appendix “B” of the IPC *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*.

The privacy policies and procedures were reviewed in November 2016, May 2017, November 2017, August 2018, January 2019, July 2019 and continue to be reviewed at regular semi-annual privacy/security review meetings. The results of these reviews were as follows:
<table>
<tr><th>Review Date</th><th>Recommendations</th><th>Actions</th><th>Action Completed</th></tr>
<tr><td>Nov 2016</td><td>New policy regarding remote network access: All approved request for remote access to be scanned and saved in “Signed Requests” archive. The maximum authorized duration of remote access rights shall be three (3) months, whereupon any extension must be authorized again in accordance with the policy.</td><td>New policy added to the policies and procedures manual. Inspirata to implement by next review date.</td><td>May 2017 Verified by Inscyte.</td></tr>
<tr><td></td><td>Existing policy in respect of conducting security audits: amended to require security scans at minimum every three (3) months.</td><td>Inspirata to implement by next review date.</td><td>May 2017 Verified by Inscyte.</td></tr>
<tr><td>May 2017</td><td>Existing policy in respect of conducting security audits: amended to</td><td>Inspirata to implement by next review date.</td><td>Nov 2017 Verified by Inscyte.</td></tr>
</table>
</td></tr>
</table>



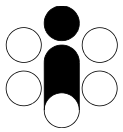
Categories	Privacy Indicators			
		require external network vulnerability scans at minimum every three (3) months.		
		Existing policy and procedure regarding patch management: amended procedure to use Windows Server Update Services software (WSUS) to automate and manage the distribution of software patches and hot fixes.	Inspirata to implement WSUS by next review date.	Nov 2017 Verified by Inscyte.
		Other recommendation: review business continuity plan every quarter and keep it up to date.	Inspirata to implement by next review date.	Nov 2017 Verified by Inscyte.
	Nov 2017	No recommendations.	N/A	N/A
	Aug 2018	No recommendations.	N/A	N/A
	Jan 2019	No recommendations.	N/A	N/A
	July 2019	Existing policy in respect of conducting security audits: amend to require scans of all internal network workstations and servers rather than random spot-audits.	Inspirata to implement by next review date.	Pending
	Each amended and/or new policy procedure was communicated to Inscyte's Agent Inspirata on the date/time of each joint review meeting through written minutes and action items recorded at each meeting. No changes were recommended or made to privacy policies as a result of the above reviews. Consequently, communication materials available to the public or other stakeholders were not amended as a result of these reviews.			

Categories	Privacy Indicators
	The next review or privacy/security procedures and practices is scheduled for December 2019.
Collection	Since the last review by the IPC in 2016 no data linkages with third parties were performed and no new data linkages were contemplated. As a result, CytoBase consist of one data holding, namely, cervical cancer screening reports performed by laboratories participating in the CytoBase program. These cervical cancer screening reports consist of: CytoBase Database — This is the main CytoBase database. CytoBase RFC — Manual change requests (data corrections). Archived HL7 Logs — Archived report transmission logs on CD/DVDs. These are held in accordance with the Statement of Purpose, Collection, Use, and Retention for CytoBase. CytoBase is the only data holding and no amendments have been made to the purpose of this holding since the last review by the IPC. This data holding has been reviewed by Inscyte since the last review by the IPC.
Use	Inscyte Corp. has no employees that work with CytoBase patient-level data. Inspirata acts as Agent for Inscyte with respect to the day-to-day operations and maintenance of CytoBase. Only designated members of Inspirata staff are permitted to work with the information in CytoBase and are limited to specific and restricted roles. These roles do not permit use of CytoBase PHI for research purposes. At the time of writing eight (8) staff members of Inspirata were authorized to work with CytoBase patient-level data. Aggregated statistics can be produced from CytoBase data. However, no statistical publications have been made since the last IPC review in 2016. Further, no requests for use of CytoBase PHI for research purposes were received or granted since the last review by the IPC.
Transfer and Disclosure	Inscyte Corporation discloses personal health for non-research purposes to the following entities under the terms and conditions of their respective data sharing agreements: 1. Patient test results are disclosed to Ontario Health on a daily basis for the purposes of the Ontario Cervical Cancer Screening Program. 2. Patient test results are disclosed on an ad-hoc real-time basis to participating medical laboratories for the purpose of



Categories	Privacy Indicators
	improving quality in the interpretation of new test specimens and for ensuring patients with abnormal screening results are followed-up appropriately. 3. Patient test results are disclosed ad-hoc to registered authorized users of the "CytoBase for Clinicians" online service for the purpose of improving patient care. Outside of the above modalities, no other requests for the disclosure of personal health information for non-research purposes were received by Inscyte since the last IPC review in 2016. No new third-party data sharing agreements have been executed since the IPC review in 2016. Inscyte did not receive requests for disclosure of personal health information for research purposes, and no disclosures of personal health information have been made for research purposes since the last IPC review in 2016. Inscyte did not receive requests for aggregate and/or de-identified information and has not disclosed aggregate or de-identified information for research since the last IPC review in 2016 and has not entered into any research agreements. As there were no disclosures of aggregate and/or de-identified information, Inscyte has had no acknowledgements or agreements from persons to whom such information was disclosed since the last review by IPC in 2016.
Data Sharing Agreements	Inscyte Corp. has the following data sharing agreements in place for the collection, use and disclosure of personal health information (there is only one agreement in effect per organization). **Laboratories (collection & transfer)** 1. LifeLabs 2. Dynacare Health 3. Medical Laboratories of Windsor These agreements have not changed since the IPC review of 2016 and remain in effect. **Healthcare Service Providers (disclosure/use)**

Categories	Privacy Indicators
	1. Ontario Health The data sharing agreement with Ontario Health has not changed since the IPC review of 2016 and remains in effect. No new data sharing agreements have been executed between Inscyte and third parties since the last review by the IPC in 2016.
Agreements with Third Party Service Providers	Inscyte Corp. has a contractual agreement in place with **Inspirata Canada Inc.** for the on-going operations and maintenance of the CytoBase database and data collection network. This agreement has not changed since the last IPC review in 2016. This is the only third-party service agreement that Inscyte Corporation has in effect.
Data Linkage	No data linkages have been performed, requested or approved since the last review by the IPC in 2016.
Privacy Impact Assessments	The most recent Privacy Impact Assessment (PIA) was conducted and completed October 31, 2013. This PIA focused on the CytoBase system and database. No recommendations for changes were made as the privacy and security controls, policies and procedures in place were deemed adequate and appropriate. Review of the existing Privacy Impact Assessment was conducted at each semi-annual privacy and security review meeting in November 2016, May 2017, November 2017, August 2018, January 2019, July 2019. After each review a determination was made that further PIAs were not required as the operational infrastructure of CytoBase, and the collection, use and disclosure of CytoBase information had not changed and did not warrant a new or revised PIA. AS such, since the las review by IPC in 2016: • No new PIAs were completed • No PIAs were undertaken but not completed • No new PIAs have been scheduled



<table>
<tr>
<td>Privacy Audit Program</td>
<td>
Inscyte's policies require a privacy program audit to be performed at least on an annual basis. Since the last review by the IPC in 2016, formal privacy/security reviews have been implemented; scheduled semi-annually, usually in November and May, with recorded minutes, recommendations, and action items. Each meeting agenda includes review of the following items:

1. Log of Data Holdings
2. Log of Authorized Personnel
3. Log of Authorized Access to PHI
4. Physical Access Logs
5. Password Policies
6. Log of Privacy Complaints
7. Log of Privacy Breaches
8. Log of Security Breaches
9. Log of PHI Transfers
10. Log of Privacy Training
11. Log of System Configuration Changes (Patch Management)
12. Data Sharing Agreements
13. Staff Confidentiality Agreements
14. Risk Register (review/identification/resolution of risks)
15. Business Continuity (Disaster Recovery)
16. Requirements for updates to TRA/PIA
17. Requirements for updates to Data Sharing and Third-Party Agreements
18. Consolidated Log of Recommendations (action items)

Reviews of agents granted approval to access and use PHI were conducted by Inscyte and its agent Inspirata in November 2016, May 2017, November 2017, August 2018, January 2019, July 2019 and continue to be reviewed at regular semi-annual privacy/security review meetings. The results of these reviews were as follows:

Audits of Agents Granted Approval to Access and Use PHI
<table>
<tr><th>Review Date</th><th>Recommendations</th><th>Actions</th><th>Action Completed</th></tr>
<tr><td>Nov 2016</td><td>No recommended changes.</td><td>N/A</td><td>N/A</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>May 2017</td><td>No recommended changes.</td><td>N/A/</td><td>N/A/</td></tr>
</table>
</td>
</tr>
</table>

Nov 2017	No recommended changes.	N/A	N/A
Aug 2018	No recommended changes.	N/A	N/A
Jan 2019	No recommended changes.	N/A	N/A
July 2019	No recommended changes.	N/A	N/A

No other privacy audits were conducted since the las review by IPC in 2016.

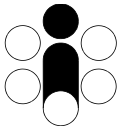
Other than Inspirata, there are no other agents granted approval to access and use personal health information. Further, Inscyte's agent Inspirata is not granted approval to access and use personal health information; rather, certain designated staff of Inspirata are permitted to access PHI only as necessary for purposes of troubleshooting, quality control and system maintenance of CytoBase.

Recommendations resulting in changes to policies and procedures are reflected in updates to Inscyte's "Privacy & Security Policies and Procedures Manual" and are communicated to its Agent Inspirata by the privacy officer and security officer via email notification and at the next scheduled privacy/security training and awareness session (held quarterly). The date of notification is noted in the policy description as the new or updated policy came into effect (the effective date).

Inscyte's Agent Inspirata performs a privacy spot-audit every month to monitor and detect potential breaches of privacy within its operating environment. The audit program consists of scanning randomly selected workstations, laptops, and servers on a monthly basis to detect healthcare related data containing patient identifiers which may have been inadvertently stored in inappropriate locations. In addition to audits of workstation and server data files, Inspirata technicians also review server process logs and firewall activity logs on a weekly basis to detect intrusion attempts and potential breaches of security or privacy.

A log is maintained of all computer scans, the date of the scan, the person performing the scan and the results of the scan.

The results of the above privacy audits have revealed no significant vulnerabilities or breaches of privacy that would require specific recommendations or actions to be taken. The results are reviewed at semi-annual privacy/security review meetings to decide on measures to



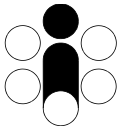
	be taken, if any, and are recorded in the recommendations and actions items of the minutes of the meeting.
Privacy Breaches	Inscyte Corp. has not received any notifications of privacy breaches or suspected privacy breaches since the last review by the IPC in 2016.
Privacy Complaints	Inscyte Corp. has not received any privacy complaints since the last review by the IPC in 2016.

Part 2 – Security Indicators

<table>
<tr><th>Categories</th><th>Security Indicators</th></tr>
<tr><td>General Security Policies and Procedures</td><td>
Inscyte Corporation has a consolidated set of policies and procedures that apply to Inscyte Corporation, and by extension, Inspirata since Inspirata acts as Agent for Inscyte in respect to CytoBase.

The “Privacy & Security Policies and Procedures Manual” addresses the requirements in Appendix “B” of the IPC *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*.

The security policies and procedures were reviewed in November 2016, May 2017, November 2017, August 2018, January 2019, July 2019 and continue to be reviewed at regular semi-annual privacy/security review meetings. The following is a summary of recommendations made, communicated to Inspirata and actioned since the last IPC review.
<table>
<tr><th>Review Date</th><th>Recommendations</th><th>Actions</th><th>Action Completed</th></tr>
<tr><td>Nov 2016</td><td>New policy regarding remote network access: All approved request for remote access to be scanned and saved in “Signed Requests” archive. The maximum authorized duration of remote access rights shall be three (3) months, whereupon any extension must be authorized again in accordance with the policy.</td><td>New policy added to the policies and procedures manual. Inspirata to implement by next review date.</td><td>May 2017 Verified by Inscyte.</td></tr>
<tr><td></td><td>Existing policy in respect of conducting security audits: amended to require security scans at minimum every three (3) months.</td><td>Inspirata to implement by next review date.</td><td>May 2017 Verified by Inscyte.</td></tr>
<tr><td>May 2017</td><td>Existing policy in respect of conducting security audits: amended to require external network</td><td>Inspirata to implement by next review date.</td><td>Nov 2017 Verified by Inscyte.</td></tr>
</table>
</td></tr>
</table>



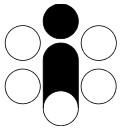
Categories	Security Indicators			
		vulnerability scans at minimum every three (3) months.		
		Existing policy and procedure regarding patch management: amended procedure to use Windows Server Update Services software (WSUS) to automate and manage the distribution of software patches and hot fixes.	Inspirata to implement WSUS by next review date.	Nov 2017 Verified by Inscyte.
		Other recommendation: review business continuity plan every quarter and keep it up to date.	Inspirata to implement by next review date.	Nov 2017 Verified by Inscyte.
	Nov 2017	No recommendations.	N/A	N/A
	Aug 2018	No recommendations.	N/A	N/A
	Jan 2019	No recommendations.	N/A	N/A
	July 2019	Existing policy in respect of conducting security audits: amend to require scans of all internal network workstations and servers rather than random spot-audits.	Inspirata to implement by next review date.	Pending
	Each amended and/or new policy procedure was communicated to Inscyte's Agent Inspirata on the date/time of each joint review meeting through written minutes and action items recorded at each meeting. Inscyte's Privacy & Security Policies and Procedures manual was last amended on May 26, 2017 for internal distribution to its Agent Inspirata. It was deemed that the changes to the security policies and procedures did not materially affect the public or other stakeholders.			

<table>
<tr><th>Categories</th><th>Security Indicators</th></tr>
<tr><td></td><td>Consequently, communication materials available to the public or other stakeholders were not amended as a result of these reviews.

The next review or privacy/security procedures and practices is scheduled for December 2019.</td></tr>
<tr><td>Physical Security</td><td>Inscyte's agent Inspirata monitors and reviews computerized logs of physical access to premises and locations within premises that contain personal health information. These logs are reviewed at minimum on a monthly basis, but in practice on a weekly basis. In the event that a breach of security is detected or suspected, Inscyte's policies require the breach to be contained and reported to the Security Officer and Privacy Officer at the first available opportunity.

Reviews of agents granted access to the premises and locations within the premises where records of personal health information are retained are carried out on a semi-annual basis by Inscyte and its agent Inspirata. Since the last review by IPC in 2016, review meetings were held in November 2016, May 2017, November 2017, August 2018, January 2019, July 2019.

Review of Agents Granted Access to Premises
<table>
<tr><th>Review Date</th><th>Recommendations</th><th>Actions</th><th>Action Completed</th></tr>
<tr><td>Nov 2016</td><td>No recommended changes.</td><td>N/A</td><td>N/A</td></tr>
<tr><td>May 2017</td><td>No recommended changes.</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Nov 2017</td><td>No recommended changes.</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Aug 2018</td><td>No recommended changes.</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Jan 2019</td><td>No recommended changes.</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Jul 2019</td><td>No recommended changes.</td><td>N/A</td><td>N/A</td></tr>
</table></td></tr>
<tr><td>Security Audit Program</td><td>While Inscyte's policies state that CytoBase system control logs and audit logs shall be reviewed on a monthly basis, we have since moved to automated processes for real-time monitoring of system controls, audit logs, and network activity to trigger alerts of unusual activity or degradation in performance.</td></tr>
</table>

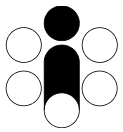


<table>
<tr><th>Categories</th><th>Security Indicators</th></tr>
<tr><td></td><td>
Inscyte's policies require that the security program be reviewed at least once per year. Since the last review by the IPC in 2016, formal privacy/security reviews have been implemented; scheduled semi-annually, usually in November and May, with recorded minutes, recommendations, and action items.
The meeting agenda includes review of the following items:

Log of Data Holdings
Log of Authorized Personnel
Log of Authorized Access to PHI
Physical Access Logs
Password Policies
Log of Privacy Complaints
Log of Privacy Breaches
Log of Security Breaches
Log of PHI Transfers
Log of Privacy Training
Log of System Configuration Changes (Patch Management)
Data Sharing Agreements
Staff Confidentiality Agreements
Risk Register (review/identification/resolution of risks)
Business Continuity (Disaster Recovery)
Requirements for updates to TRA/PIA
Requirements for updates to Data Sharing and Third-Party Agreements
Consolidated Log of Recommendations (action items)

The following is a summary of recommendations made, communicated and actioned since the last IPC review.
<table>
<tr><th>Review Date</th><th>Recommendations</th><th>Actions</th><th>Action Completed</th></tr>
<tr><td>Nov 2016</td><td>New policy regarding remote network access: All approved request for remote access to be scanned and saved in "Signed Requests" archive. The maximum authorized duration of remote access rights shall be three (3) months, whereupon any</td><td>New policy added to the policies and procedures manual. Inspirata to implement by next review date.</td><td>May 2017 Verified by Inscyte.</td></tr>
</table>
</td></tr>
</table>

Categories	Security Indicators			
		extension must be authorized again in accordance with the policy.		
		Existing policy in respect of conducting security audits: amended to require security scans at minimum every three (3) months.	Inspirata to implement by next review date.	May 2017 Verified by Inscyte.
	May 2017	Existing policy in respect of conducting security audits: amended to require external network vulnerability scans at minimum every three (3) months.	Inspirata to implement by next review date.	Nov 2017 Verified by Inscyte.
		Existing policy and procedure regarding patch management: amended procedure to use Windows Server Update Services software (WSUS) to automate and manage the distribution of software patches and hot fixes.	Inspirata to implement WSUS by next review date.	Nov 2017 Verified by Inscyte.
		Other recommendation: review business continuity plan every quarter and keep it up to date.	Inspirata to implement by next review date.	Nov 2017 Verified by Inscyte.
	Nov 2017	No recommendations.	N/A	N/A
	Aug 2018	No recommendations.	N/A	N/A
	Jan 2019	No recommendations.	N/A	N/A
	July 2019	Existing policy in respect of conducting security audits: amend to require	Inspirata to implement by next review date.	Pending



Categories	Security Indicators

	scans of all internal network workstations and servers rather than random spot-audits.		

The above recommendations were communicated to Inscyte's Agent Inspirata and were scheduled for implementation before the next semi-annual review. Recommendations resulting in changes to policies and procedures are reflected in updates to Inscyte's "Privacy & Security Policies and Procedures Manual" and are communicated to its Agent Inspirata by the privacy officer and security officer via email notification and at the next scheduled privacy/security training and awareness session (held quarterly). The date of notification is noted in the policy description as the new or updated policy came into effect (the effective date).

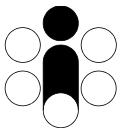
Since the last review by the IPC in 2016, patches have been applied to the CytoBase computing infrastructure in accordance with Inscyte's patch management policies and procedures. This has included all Microsoft Windows patches and Oracle RDBMS as up to June 20, 2019 (at the time of writing). All patches have been logged in the Log of Configuration Changes and Patches.

In addition to semi-annual privacy/security reviews, Inspirata performs security audits on a regular basis as follows:

- Physical access logs are reviewed at minimum monthly but weekly in practice
- Internet facing firewall traffic patterns are monitored automatically
- CytoBase data transaction logs are monitored automatically
- CytoBase for Clinicians web server logs are monitored automatically
- CytoBase for Clinicians user activity logs are monitored automatically
- Network activity is monitored automatically
- Network server vulnerability scans are run quarterly

The results of the above security audits have revealed no significant vulnerabilities or breaches of security that would require specific recommendations or actions to be taken. The results are reviewed at semi-annual privacy/security review meetings to decide on measures to

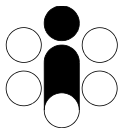
Categories	Security Indicators
	be taken, if any, and are recorded in the recommendations and actions items of the minutes of the meeting.
Information Security Breaches	Since the last review by the IPC in 2016, there have been no detected security breaches in respect of CytoBase.



Part 3 – Human Resources Indicators

Categories	Human Resource Indicators
Privacy Training and Awareness	All agents of Inscyte have received at least two privacy awareness training session per year since the prior review by the IPC, with the exception of one individual working off-site who has received one training session per year. Training sessions are conducted at Inspirata's all-staff meetings, which are scheduled on a nominally quarterly basis and cover both privacy and security matters. Communications to agents related to privacy are delivered on the dates of these meetings. Since the last review by the IPC in 2016, training sessions have been held on the following dates: February 3, 2017 26 Attendees August 4, 2017 33 Attendees October 27, 2017 35 Attendees March 29, 2018 33 Attendees October 26, 2018 33 Attendees February 15, 2019 32 Attendees May 9, 2019 29 Attendees October 25, 2019 29 Attendees Communications to agents by Inscyte in relation to privacy matters are made at the privacy training sessions. The meeting scheduled for summer of 2018 could not be held due to logistics in obtaining a meeting site and the absence of key staff due to vacations and other business commitments. There are no employees of Inspirata or Agents of Inscyte that have not received privacy and security awareness training. Eight (8) employees of Inspirata are authorized to work with CytoBase. There have been no new hires authorized to work with CytoBase since the last review by the IPC. Designated employees of Inspirata who have access to CytoBase have received at least two training sessions per year, except for one off-site individual, which could only attend one session per year in person. To fully comply with Inscyte's policies, off-site staff will be henceforth trained via online webinars to obtain at least two training session per year.

Categories	Human Resource Indicators
Security Training and Awareness	All agents of Inscyte have received at least two security awareness training session per year since the prior review by the IPC , with the exception of one individual working off-site who has received one training session per year. Training sessions are conducted at Inspirata's all-staff meetings, which are scheduled on a nominally quarterly basis, and cover both privacy and security matters. Communications to agents related to security are delivered on the dates of these meetings. Since the last review by the IPC in 2016, training sessions were held on the following dates: February 3, 2017 26 Attendees August 4, 2017 33 Attendees October 27, 2017 35 Attendees March 29, 2018 33 Attendees October 26, 2018 33 Attendees February 15, 2019 32 Attendees May 9, 2019 29 Attendees October 25, 2019 29 Attendees Communications to agents by Inscyte in relation to security matters are made at the security training sessions. The meeting scheduled for summer of 2018 could not be held due to difficulty in obtaining a meeting site and the absence of significant staff due to vacations and other business commitments. There are no employees of Inspirata or Agents of Inscyte that have not received privacy and security awareness training. Eight (8) employees of Inspirata are authorized to work with CytoBase. There have been no new hires authorized to work with CytoBase since the last review by the IPC in 2016. Designated employees of Inspirata who have access to CytoBase have received at least two training sessions per year, except for one off-site staff, which could only attend one session per year in person. To fully comply with Inscyte's policies, off-site staff will be henceforth trained via online webinars to obtain at least two training session per year.
Confidentiality Agreements	All agents of Inscyte (including all employees of Inspirata) as a condition of employment or contract, execute a signed and witnessed "Personal Health Information Confidentiality and Non-Disclosure Agreement" with respect to the handling of personal health



Categories	Human Resource Indicators
	information. There are no Agents of Inscyte who have not executed a confidentiality agreement. These agreements refer to the Act as the prevailing legislation, the privacy & security policies and procedures, and stipulate the consequences of breach. At present all employees of Inscyte's Agent Inspirata have executed agreements. These agreements are not currently re-executed on an annual basis; however, all agents are reminded of their signed agreements and obligations at Privacy & Security Awareness training sessions.
Termination or Cessation	No notifications of termination have been received by Inscyte Corporation from its Agent Inspirata with respect to the termination of employment of an individual assigned to work with CytoBase as such terminations have not occurred since the last review by the IPC in 2016.

Part 4 – Organizational Indicators

Categories	Organizational Indicators
Risk Management	Inscyte Corporation's policy states that the risk register will be reviewed at least once per year. Since the last review by the IPC in 2016, semi-annual privacy/security review meetings have been established at which the risk register is reviewed. In addition, Inscyte's Agent Inspirata, reviews risk to CytoBase on an on-going basis at weekly technical support departmental meetings. The corporate risk register was reviewed at each semi-annual privacy/security review meeting in November 2016, May 2017, November 2017, August 2018, January 2019, and July 2019. The risk register is updated as required. Since the last review by the IPC in 2016, the risk register was updated in June 2018 as follows: • Security Risk: disclosure (hacking) due to older network encryption. Addressed with upgrade to NIST compliant advanced encryption standard (AES-256) in network transmissions from all laboratories completed November 2017.

Categories	Organizational Indicators
	• Availability Risk: Risk of loss of Internet Service Provider outage. Risk of outage on uninterruptible power supply units. Probability low but impact is high. Logged June 2018. Work with Internet service providers is in progress to mitigate this risk.
Business Continuity and Disaster Recovery	Inspirata's corporate disaster recovery plan incorporates the recovery of Inscyte Corporation's CytoBase system since it is hosted on Inspirata's computing infrastructure. Inspirata's disaster recovery plan is updated on an on-going basis in conjunction with infrastructure modifications, upgrades, or expansions. Updated versions of the disaster recovery plan were published internally on February 6, 2017 and on August 1, 2018. Changes to the disaster recovery plan consisted of updated technical specifications and configurations of hardware and software for the CytoBase system, as well as backup images of virtual severs. No tests of the disaster recovery plan were conducted since the last review by the IPC in 2016, and no changes have been made to the disaster recovery plan as a result of such tests.