Inscyte Corporation

Privacy & Security Policies and Procedures Manual

Date: May 26, 2017

Revision 4.0

Table of Contents

Important Information about Privacy & Security

The Law in Ontario

The **Personal Health Information Protection Act, 2004** ("the Act") is an Ontario provincial law that governs the collection, use and disclosure of personal health information within the health care system. The objective is to keep personal health information confidential and secure, while allowing for the effective delivery of health care services. Under this legislation, health care providers and others who deliver health care services are collectively known as "health information custodians."

The purposes of the Act are,

(a) to establish rules for the collection, use and disclosure of personal health information about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information, while facilitating the effective provision of health care;
(b) to provide individuals with a right of access to personal health information about themselves, subject to limited and specific exceptions set out in this Act;
(c) to provide individuals with a right to require the correction or amendment of personal health information about themselves, subject to limited and specific exceptions set out in this Act;
(d) to provide for independent review and resolution of complaints with respect to personal health information; and
(e) to provide effective remedies for contraventions of this Act. 2004, c. 3, Sched. A, s. 1.

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

One such disclosure that is permitted without consent is the disclosure of personal health information to prescribed persons that compile or maintain registries of personal health information for purposes of facilitating or improving the provision of health care or that relate to the storage or donation of body parts or bodily substances pursuant to subsection 39(1)(c) of the Act.

Another such disclosure that is permitted without consent is the disclosure of personal health information to prescribed entities for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system pursuant to section 45 of the Act.

These disclosures are permitted without consent provided that the prescribed persons and prescribed entities comply with the requirements set out in the Act and Regulation 329/04 to the Act ("regulation").

In order for a health information custodian to be permitted to disclose personal health information to a prescribed person or prescribed entity without consent, the prescribed person or prescribed entity must have in place practices and procedures approved by the Information and Privacy Commissioner of Ontario to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. In the case of a prescribed person, this requirement is set out in subsection 13(2) of the regulation to the Act. In the case of a prescribed entity, this requirement is set out in subsection 45(3) of the Act.

These practices and procedures are reviewed by the Information and Privacy Commissioner of Ontario every three years from the date of their initial approval in order for a health information custodian to be able to continue to disclose personal health information to a prescribed person or prescribed entity without consent and in order for the prescribed person or prescribed entity to be able to continue to collect, use and disclose personal health information without consent as permitted by the Act and the regulation to the Act. In the case of a prescribed person, this requirement is set out in subsection 13(2) of the regulation to the Act. In the case of a prescribed entity, this requirement is set out in subsection 45(4) of the Act.

About Inscyte Corporation

Inscyte Corporation is a not-for-profit partnership of Ontario medical laboratories and Cancer Care Ontario (CCO). 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 specific 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 Cancer Care Ontario (CCO). Screening test results received from participating laboratories are forwarded to CCO on a daily basis for incorporation into CCO'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 characteristics 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 or nurse practitioners to access screening histories and follow-up status only on individual patients within their care.

Ontario Regulation 329/04 designates Inscyte Corporation in respect of CytoBase as a Prescribed Person pursuant to subsection 39(1)(c) of the Act.

About Artificial Intelligence In Medicine Inc.

Inscyte Corporation has contracted AIM 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 AIM's secure datacenter. AIM 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.

As such, AIM is considered an "Agent" of Inscyte Corporation and must implement security policies and procedures that ensure that Inscyte Corporation meets its obligations with respect to its designation as a Prescribed Person under the Act.

Since AIM 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, AIM privacy and security program implements Inscyte Corporation's Privacy & Security Policies and Procedures.

Important Information about this Manual

Scope of Applicability

This Privacy & Security Policies and Procedures Manual is the official statement of Inscyte Corporation's privacy and security program. Since AIM is an Agent of Inscyte Corporation, and Inscyte is a Prescribed Person under Ontario's Personal Health Information Protection Act, 2004, these policies and procedures apply to AIM as well. Unless otherwise stated, all procedures and policies articulated herein are applicable to both the staffs of Inscyte and AIM.

This manual supersedes all previous manuals and protocols, specifically:

- Inscyte Corporation Privacy Protocols and Procedures, Rev 1.0 September 28, 2005
- Inscyte Corporation Privacy Protocols and Procedures, Rev 2.0 August 14, 2008
- AIM Inc. Privacy Protocols and Procedures, Rev 3.0, September 9, 2005
- AIM Inc. Privacy Protocols and Procedures, Rev 4.0, May 23, 2008

Verb Usage

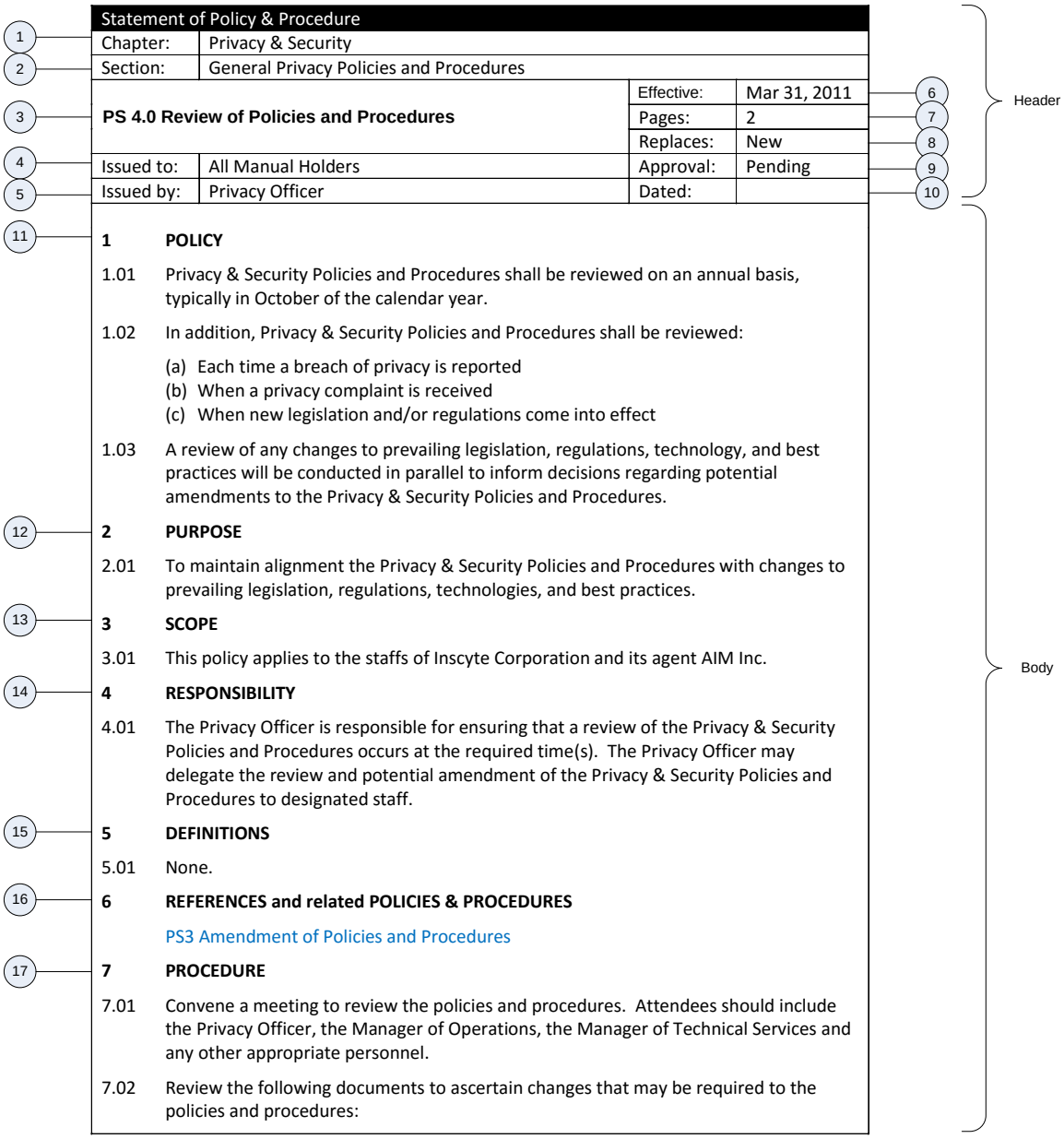
Statements containing "shall" are used for binding requirements that must be verified and have an accompanying method of verification; "will" is used as a statement of fact, declaration of purpose, or expected occurrence; "should" denotes a statement of best practice; and "may" means a potential of occurrence.

List of Abbreviations

Abbreviation	Meaning
AIM	Artificial Intelligence In Medicine Inc. – a Toronto based software engineering company that designed and operates the CytoBase system.
CCO	Cancer Care Ontario – a provincial agency responsible for improving cancer services and advising government on matters concerning cancer prevention and treatment.
IPC	The Office of the Information and Privacy Commissioner Ontario
PHI	Personal Health Information
VPN	Virtual Private Network
WAP	Wireless Access Point

Format of Policy & Procedures Documentation

Each policy is described in a *Statement of Policy and Procedure Card* as shown below.



Statement of Policy & Procedure			
1 Chapter:	Privacy & Security		
2 Section:	General Privacy Policies and Procedures		
3 **PS 4.0 Review of Policies and Procedures**		Effective:	Mar 31, 2011
		Pages:	2
		Replaces:	New
4 Issued to:	All Manual Holders	Approval:	Pending
5 Issued by:	Privacy Officer	Dated:	

6 7 8 9 10 Header

11 **1 POLICY**

1.01 Privacy & Security Policies and Procedures shall be reviewed on an annual basis, typically in October of the calendar year.

1.02 In addition, Privacy & Security Policies and Procedures shall be reviewed:

(a) Each time a breach of privacy is reported
(b) When a privacy complaint is received
(c) When new legislation and/or regulations come into effect

1.03 A review of any changes to prevailing legislation, regulations, technology, and best practices will be conducted in parallel to inform decisions regarding potential amendments to the Privacy & Security Policies and Procedures.

12 **2 PURPOSE**

2.01 To maintain alignment the Privacy & Security Policies and Procedures with changes to prevailing legislation, regulations, technologies, and best practices.

13 **3 SCOPE**

3.01 This policy applies to the staffs of Inscyte Corporation and its agent AIM Inc.

14 **4 RESPONSIBILITY**

4.01 The Privacy Officer is responsible for ensuring that a review of the Privacy & Security Policies and Procedures occurs at the required time(s). The Privacy Officer may delegate the review and potential amendment of the Privacy & Security Policies and Procedures to designated staff.

15 **5 DEFINITIONS**

5.01 None.

16 **6 REFERENCES and related POLICIES & PROCEDURES**

PS3 Amendment of Policies and Procedures

17 **7 PROCEDURE**

7.01 Convene a meeting to review the policies and procedures. Attendees should include the Privacy Officer, the Manager of Operations, the Manager of Technical Services and any other appropriate personnel.

7.02 Review the following documents to ascertain changes that may be required to the policies and procedures:

Body

The card consists of an administrative header section and the body (description) of the policy. The elements of the card are described below in terms of the numbered items.

1. The **Chapter** refers to a major section of the corporate policy and procedure manual.
2. The **Section** refers to a sub-section of a chapter.
3. Each Policy is uniquely identified by a **policy number and subject**. The number is in the format <prefix><number.version>. The prefix in the example is “PS” which represents

"privacy & security". In the example, this is policy number is "4.0". As amendments are made to this policy the number would be incremented as "4.1", "4.2" and so on for each amendment.

4. **Issued to** refers to the staffs or groups of staffs to whom the policies have been or will be distributed.
5. **Issued by** is the name of the authority who issued the policy. With respect to privacy and security policies this is usually the Privacy Officer.
6. **Effective** is the date that the policy took effect. This date can be a future "target" date as new policies are prepared.
7. **Pages** denotes the number of pages in the manual that the policy card spans.
8. The **Replaces** field contains either the number of the policy that this policy supersedes (e.g. PS 1.2) or the literal value "New" which means that this policy did not exist previously.
9. The **Approval** field contains the initials of the person authorized to approve the policy. Approval (i.e. sign-off) is required before a policy can take effect. If a policy is awaiting approval this field should contain the literal value "Pending".
10. The **Dated** field contains the date upon which the policy was approved. This date will usually precede the Effective Date since approval should be obtained before a policy is implemented. If the approval is "Pending" this field may be left empty.
11. The body of the policy card begins with the **POLICY** section. This section contains one or more statements describing the policy. Statements of policy describe what shall or will be done with respect to the subject matter, or a statement of the philosophical position with respect to the subject matter.
12. The **PURPOSE** section contains statement describing why the policy is in place thereby establishing a context for the policy.
13. The **SCOPE** section describes to whom the policy applies or does not apply.
14. The **RESPONSIBILITY** section describes who is responsible for ensuring that the policy is carried out. This is not necessarily the same as who will actually do the related work, since those who are responsible could delegate the work to others. However, delegation of work does not absolve the delegator of the responsibility for ensuring the work is completed.
15. The **DEFINITIONS** section should contain statements that define concepts articulated in the policy whose meaning or scope may not be obvious.
16. **REFERENCES and related POLICIES** contains a list of related policies as well as external documents that provide additional contextual information about the policy. In the electronic version of the manual, these are document links that allow for easy navigation to related contextual information.
17. The **PROCEDURE** section contains a set of instructions for carrying out work to ensure compliance with the policy. If a policy is merely a statement of a philosophical position on the subject matter, then there may be no related procedure.
18. The **REVISION HISTORY** section contains information about historical changes made to the policy and procedure statement.

Revision History

Revision 4.0 May 26, 2017

Update policy 15.1 to change Security scan frequency from annual to quarterly

Revision 3.1 November 7, 2016

New policy/procedure 14.22 added addressing Remote Network Access

Update policy 12.10 to include action for revoked pass card

Revision 2.0 August 30, 2013

Revised policy/procedure PS 14.6 Requirements for Passwords to require minimum password length of 10 characters rather than the previous 8 characters, and inclusion of upper and lower case characters in password composition rules.

Revised policy/procedure PS 14.20 Requirements for Internet Applications Accessing PHI. Rule 1.03 adds the stipulation that "Standard RDBMS access ports are not to be used". New rules 1.12, 1.13, and 1.14 added addressing strengthening the security posture of Internet application servers.

Revision 1.0 September 30, 2011

Initial Final Draft

Review and Approvals

Revision	Review Date	Reviewed By	Approval Signature

1 General Privacy Policies and Procedures

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	1 General Privacy Policies and Procedures		
PS 1.1 Existence of Policies and Procedures		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte Corporation and its Agent(s) shall have formal policies and procedures in place at all times to ensure that personal health information in its possession is protected and safeguarded in accordance with prevailing legislative requirements, regulations, and best practices.

1.02 In particular, the Privacy & Security Policies and Procedures shall encompass:

(a) Status under the Personal Health Information Act, Ontario, 2004
(b) On-going review, amendment and auditing of policies and procedures
(c) Privacy and security accountability framework
(d) Collection of personal health information
(e) Use of personal health information
(f) Disclosure of personal health information
(g) Secure retention, transfer and disposal of personal health information
(h) Implementation of administrative, technical, and physical safeguards
(i) Inquiries, concerns or complaints to information practices
(j) Transparency of practices in respect of personal health information

1.03 The most current Privacy & Security Policies and Procedures Manual shall be stored on AIM's business network in PDF format and made available to all staff for viewing or download.

2 PURPOSE

2.01 **Inscyte Corporation**, with respect to **CytoBase**, is a prescribed person under the Act. This means that health information custodians can disclose personal health information to Inscyte Corporation without having to obtain the consent of individuals. It requires that Inscyte Corporation complies with the requirements of the Act.

2.02 **Artificial Intelligence In Medicine Inc.** (AIM) is a software engineering firm providing products and services to the healthcare and medical research industries. Inscyte Corporation has contracted AIM to operate and maintain the CytoBase system on a day-to-day basis. As such, **AIM is an agent of Inscyte Corporation** and must comply with these Privacy & Security Policies and Procedures to satisfy Inscyte Corporation's obligations under the Act.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and its agent AIM Inc.

4 RESPONSIBILITY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	1 General Privacy Policies and Procedures		
PS 1.1 Existence of Policies and Procedures		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

4.01 It is the responsibility of the President of Inscyte Corporation to ensure that its Agents have Privacy & Security Policies and Procedures in place that satisfy Inscyte Corporation's requirements in terms of its obligations under the Act.

4.02 It is the responsibility of the CEO of AIM to ensure that its operations are in compliance with these Privacy & Security Policies and Procedures.

5 DEFINITIONS

5.01 **Personal Health Information** is defined as follows.

Ontario's *Personal Health Information Protection Act, 2004,* defines "personal health information" as identifying information about an individual in oral or recorded form, if the information,

(a) Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
(b) Relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
(c) Is a plan of service within the meaning of the *Long-Term Care Act, 1994* for the individual,
(d) Relates to payments or eligibility for health care in respect of the individual,
(e) Relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
(f) Is the individual's health number, or
(g) Identifies an individual's substitute decision-maker.

6 REFERENCES and related POLICIES & PROCEDURES

Inscyte Corporation Privacy Code – Revision 2.0 August 2008

PS 3.1 Publication of these Policies and Procedures

PS 3.2 Privacy Document Archives

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	1 General Privacy Policies and Procedures		
PS 1.2 Review of Policies and Procedures		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Privacy & Security Policies and Procedures shall be reviewed on an annual basis, typically in October of the calendar year.

1.02 In addition, Privacy & Security Policies and Procedures should be reviewed:

(a) Each time a breach of privacy is reported
(b) When a privacy complaint is received
(c) When new legislation and/or regulations come into effect

1.03 A review of any changes to prevailing legislation, regulations, technology, and best practices should be conducted in parallel to inform decisions regarding potential amendments to the Privacy & Security Policies and Procedures.

2 PURPOSE

2.01 To maintain alignment the Privacy & Security Policies and Procedures with changes to prevailing legislation, regulations, technologies, and best practices as well as in response to breaches, complaints, or reviews by the Office of the Information and Privacy Commissioner, Ontario.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 The Privacy Officer is responsible for ensuring that a review of the Privacy & Security Policies and Procedures occurs at the required time(s).

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 1.3 Amendment of Policies and Procedures

PS 10.3 Conducting Privacy Audits

PS 11.2 Reporting a Breach of Privacy

PS 11.5 Handling Privacy Complaints

7 PROCEDURE

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	1 General Privacy Policies and Procedures		
PS 1.2 Review of Policies and Procedures		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.01 Convene a meeting (or set of meetings) to review the policies and procedures. Attendees should include the Privacy Officer, the Security Officer, the Manager of Technical Services and any other appropriate personnel.

7.02 Review the following documents to ascertain changes that may be required to the policies and procedures:

(a) The Log of Privacy Breaches
(b) The Log of Security Breaches
(c) The Log of Privacy Complaints
(d) The Corporate Risk Register
(e) Log of Individual Requests to Access PHI
(f) Log of Privacy Awareness Training Sessions
(g) Any Threat Risk Analyses performed since the last review
(h) Any Privacy Impact Assessments performed since the last review

7.03 Ascertain if any issues need to be addressed and prepare a report of recommended actions/changes to policies and procedures, privacy or security measures. Provide a copy of the report to the Privacy Officer.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	1 General Privacy Policies and Procedures		
PS 1.3 Amendment of Policies and Procedures		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 The Privacy & Security Policies and Procedures Manual shall be amended in a timely manner to comply with changes to prevailing legislation, technologies, regulations or best practices or as recommended through regular reviews of the policies and procedures, either internally, or by the Office of the Information and Privacy Commissioner, Ontario.

2 PURPOSE

2.01 To maintain alignment of the Privacy & Security Policies and Procedures with changes to prevailing legislation, regulations, technologies and best practices.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 The Privacy Officer is responsible for ensuring that appropriate amendments are made to the Privacy & Security Policies and Procedures Manual in a timely manner.

4.02 The President of Inscyte is responsible for reviewing and approving amended and new statement of policy to permit the issue of revisions to the Privacy & Security Policies and Procedures Manual.

5 DEFINITIONS

5.01 None.

6 REFERENCES and related POLICIES & PROCEDURES

PS 1.2 Review of Policies and Procedures

PS 1.4 Creating New Statements of Policy and Procedure

PS 3.1 Publication of these Policies and Procedures

7 PROCEDURE

7.01 New statements of policy and amendments to existing statements of policy may be initiated at any time as required. These changes shall be accrued to a queue of "pending changes" so that final drafts can be reviewed and forwarded for approval.

7.02 The Privacy Officer shall decide when to roll-up accrued pending changes and issue a revised Privacy & Security Policies and Procedures Manual.

8 REVISION HISTORY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	1 General Privacy Policies and Procedures		
PS 1.3 Amendment of Policies and Procedures		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	
None			

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	1 General Privacy Policies and Procedures		
PS 1.4 Creating New Statements of Policy and Procedure		Effective:	Nov 1, 2011
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 New Statements of Policy and Procedure shall be created when there is evidence that the existing framework of Privacy & Security Policies and Procedures is deficient with respect to scope and/or clarity.

1.02 New Statements of Policy and Procedure shall be reviewed and approved by the President prior to being published and taking effect.

2 PURPOSE

2.01 To maintain alignment of the Privacy & Security Policies and Procedures with changes to prevailing legislation, regulations, technologies and best practices.

2.02 To establish consistent methods of identification, formatting, description, approval and publication of statements of policy and procedure.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 The Privacy Officer is responsible for ensuring that new Statements of Policy and Procedure are created and issued in a timely manner.

5 DEFINITIONS

5.01 A Statement of Policy and Procedure is comprised of the following administrative elements, all of which are mandatory.

Chapter:	The name of the chapter to which the statement applies.
Section:	The name of the section to which the statement applies.
ID:	A unique number for each statement in the form PS N.R where N is the statement ID number and R is the revision number (0,1,2…) The prefix PS denotes “Privacy & Security”.
Title:	The statement title.
Effective:	The date when the policy statement takes effect.
Pages:	The number of pages that the statement occupies.
Replaces:	Contains the ID of the statement that is superseded by the new or amended statement (if any), otherwise “New”.
Issued to:	The audience to which the statement applies.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	1 General Privacy Policies and Procedures		
PS 1.4 Creating New Statements of Policy and Procedure		Effective:	Nov 1, 2011
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

Issued by: The authority who issued the statement.

Approval: The initials of the authority who approved the statement.

Dated: The date of approval.

In addition, each statement of policy and procedure is described in terms of the following seven headings:

1 Policy: A concise statement of the policy.

2 Purpose A clear description of the reason(s) for issuing the policy and associated procedures.

3 Scope A list of entities to whom the policy applies and conditions (if any) under which the policy applies.

4 Responsibility The persons who are responsible for ensuring the policy and procedures are followed.

5 Definitions Definitions of related terms or concepts (if any).

6 References A list of citations to supporting documentation and related policies and procedures.

7 Procedure Instructions for carrying out work related to the policy.

8 Revision Hx The historical changes made to the policy.

6 REFERENCES and related POLICIES & PROCEDURES

PS 1.3 Amendment of Policies and Procedures

PS 1.5 Amending Statements of Policy and Procedure

PS 3.1 Publication of these Policies and Procedures

7 PROCEDURE

7.01 Access AIM's privacy document archives to obtain a template Statement of Policy and Procedure Card (in Microsoft Word format).

7.02 Compose the new statement of policy and store it in the "Pending Changes" sub folder.

7.03 Forward a copy of the new statement to the Privacy Officer for review.

7.04 When a final draft is completed, forward a copy to the President of Inscyte for approval.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	1 General Privacy Policies and Procedures		
PS 1.4 Creating New Statements of Policy and Procedure		Effective:	Nov 1, 2011
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	1 General Privacy Policies and Procedures		
PS 1.5 Amending Statements of Policy and Procedure		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Existing Statements of Policy and Procedure shall be amended when there is evidence that a policy/procedure is deficient with respect to scope and/or clarity.

1.02 Amended Statements of Policy and Procedure shall be reviewed and approved by the President of Inscyte prior to being published and taking effect.

2 PURPOSE

2.01 To ensure that changes to policies and procedures are controlled and approved.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 The Privacy Officer is responsible for ensuring that Statements of Policy and Procedure are amended as required in a timely manner.

4.02 It is the responsibility of the President of Inscyte Corporation to review and approve amended Statements of Policy and Procedure in a timely manner.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 1.3 Amendment of Policies and Procedures

PS 1.4 Creating New Statements of Policy and Procedure

PS 3.1 Publication of these Policies and Procedures

7 PROCEDURE

7.01 Access AIM's privacy document archives to obtain a copy of the Statement of Policy and Procedure Card to be amended.

7.02 Modify the statement ensuring to increment the policy revision number.

7.03 Store the amended statement in the "Pending Changes" sub folder.

7.04 Forward a copy of the new statement to the Privacy Officer for review.

7.05 When a final draft is completed, forward a copy to the President of Inscyte for approval.

8 REVISION HISTORY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	1 General Privacy Policies and Procedures		
PS 1.5 Amending Statements of Policy and Procedure		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	
None			

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	1 General Privacy Policies and Procedures		
PS 1.6 Transparency of Policies and Procedures		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte Corporation shall make the following information freely available to the public:

a) Privacy Code
b) Privacy & Security Policies and Procedures
c) Privacy Brochure
d) Answers to Frequently Asked Questions
e) Letters from the Information and Privacy Commissioner of Ontario regarding Inscyte's status and review as a prescribed person under the Act
f) Updated list of data holdings
g) Summary of privacy impact assessments
h) Name, title and contact information of the agent(s) to whom inquiries, concerns, complaints and requests regarding Inscyte's privacy policies and compliance under the Act are to be directed

1.02 The above information shall be easily accessed and made available for viewing and/or download from Inscyte Corporation's website.

1.03 Inscyte's Privacy Brochure shall contain the following information at minimum:

a) The status of Inscyte Corporation under the Act
b) Inscyte's obligations under the Act
c) The type of personal health information collected
d) The organizations from which personal health information is collected
e) The purpose for which personal health information is collected
f) The purpose for which personal health information is used
g) The circumstances under which personal health information is disclosed
h) The entities to whom personal information is disclosed
i) 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
j) 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

2 PURPOSE

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	1 General Privacy Policies and Procedures		
PS 1.6 Transparency of Policies and Procedures		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

2.01 Inscyte Corporation is a prescribed person under Ontario's *Personal Health Information Protection Act, 2004*. Transparency and disclosure of Inscyte Corporation's privacy policies, procedures and practices is required under the Act.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 The President of Inscyte Corporation is responsible for ensuring that its status under the Act and its privacy policies, procedures and practices are available to the public.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

Personal Health Information Protection Act, 2004, Ontario

Ontario Regulation 329/04 in respect of the Act

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

2 Governance and Accountability

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	2 Governance and Accountability		
PS 2.1 Governance Framework		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A Privacy and Security governance and accountability framework shall be established and documented that stipulates:

a) The title of the person(s) who is/are ultimately accountable for all privacy and security matters
b) The positions that have been delegated day-to-day authority to manage the privacy and security programs
c) The role of the Board of Directors in the privacy program and the frequency of updates about privacy matters at the board level
d) The agent(s) responsible for communicating such updates
e) An organizational chart describing the positions and roles in the privacy program

1.02 The governance and accountability framework shall be described in a "**Privacy and Security Governance Framework**" document.

1.03 The document shall be revised as required and previous copies shall be archived for future reference.

2 PURPOSE

2.01 Inscyte Corporation is a prescribed person under Ontario's *Personal Health Information Protection Act, 2004*. A privacy and security governance framework is a required component of a compliant privacy and security program under the Act.

2.02 AIM is a software engineering company that works in the healthcare domain. AIM performs work on behalf of health information custodians and is an agent of Inscyte Corporation, under contract for the day-to-day operations of CytoBase. As such, AIM must implement a security governance framework for its privacy and security program.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the CEO of Inscyte Corporation to ensure that Inscyte has a privacy and security governance and accountability framework in place.

4.02 It is the responsibility of the CEO of AIM to ensure that AIM has a privacy and security governance and accountability framework in place that complies with the requirements of Inscyte Corporation.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	2 Governance and Accountability		
PS 2.1 Governance Framework		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

4.03 Changes to the Privacy and Security Governance Framework is the responsibility of the CEO of AIM jointly with the CEO of Inscyte Corporation.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 2.2 Accountability for Privacy & Security

PS 2.3 Terms of Reference

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	2 Governance and Accountability		
PS 2.2 Accountability for Privacy & Security		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 The CEO of Inscyte Corporation is ultimately accountable for all matters concerning privacy and security within the scope of Inscyte's operations and is accountable for Inscyte's compliance with the Act.

1.02 The CEO of AIM is ultimately accountable for all matters concerning privacy and security within the scope of AIM's operations and is accountable for implementing privacy and policy programs that meet Inscyte Corporations requirements.

2 PURPOSE

2.01 Inscyte Corporation is a prescribed person under Ontario's *Personal Health Information Protection Act, 2004*. Accountability is a required component of a compliant privacy and security program under the Act.

2.02 AIM is a software engineering company that works in the healthcare domain. AIM performs work on behalf of health information custodians and is an agent of Inscyte Corporation, under contract for the day-to-day operations of CytoBase. As such, AIM must also demonstrate accountability for its privacy and security program.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 The CEO of AIM and the CEO of Inscyte Corporation are responsible for this statement of policy.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 2.1 Governance Framework

PS 2.3 Terms of Reference

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	2 Governance and Accountability		
PS 2.3 Terms of Reference		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte Corporation's Privacy and Security Program is managed by AIM Inc. under the direction of Inscyte's Privacy Officer.

1.02 Inscyte's Privacy Officer reports to the President of Inscyte.

1.03 The President of Inscyte reports to the Board of Directors of Inscyte Corporation.

1.04 AIM's Privacy and Security Program (in support of Inscyte) is managed by AIM's Privacy Officer and the Security Officer.

1.05 AIM's Privacy Officer reports to the CEO of AIM Inc.

1.06 AIM's Security Officer reports to the CEO of AIM Inc.

1.07 AIM's Privacy Officer and Security Officer are members of AIM's management committee and are responsible for bringing forward all issues regarding privacy and security before the committee for resolution.

1.08 AIM's management committee's role is to advise and make decisions regarding all business related matters including privacy and security issues, audits, and the management of privacy breaches, inquiries and complaints. The committee meets weekly and reports relevant matters to the Privacy Officer and President of Inscyte on an ad-hoc basis.

1.09 The President of Inscyte informs the Board of Directors of Inscyte about privacy and security matters.

2 PURPOSE

2.01 To provide a statement describing the terms of reference in the governance and management of the privacy and security program of Inscyte Corporation and in relation to its Agent, AIM Inc.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 The CEO of AIM and the CEO of Inscyte Corporation are responsible for this statement of policy.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	2 Governance and Accountability		
PS 2.3 Terms of Reference		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 2.1 Governance Framework

PS 2.2 Accountability for Privacy & Security

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

3 Implementation of Policies and Procedures

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.1 Publication of these Policies and Procedures		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 The Privacy & Security Policies and Procedures Manual shall be posted on AIM's business network in PDF format accessible to all staff.

1.02 Whenever amendments are made to the policies and procedures all staff shall be notified by email that an updated version of the documentation is available. This notification shall include a summary of revisions made and a reference to the storage location of the updated manual.

1.03 Changes to policies and procedures will also be reviewed at each of AIM's quarterly meetings and in conjunction with regular privacy awareness training sessions.

1.04 Whenever amendments are made a copy of the updated Privacy & Security Policies and Procedures Manual shall also be forwarded to Inscyte Corporation and posted on Inscyte's website.

2 PURPOSE

2.01 To ensure that all affected parties and personnel are aware of Privacy & Security Policies and Procedures and have ready access to the latest documentation.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that updates to the policies and procedures are published and communicated to all affected parties.

4.02 The Privacy Officer may delegate the work of publication and notification to designated staff.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 1.3 Amendment of Policies and Procedures

PS 3.2 Privacy Document Archives

7 PROCEDURE

7.01 None

8 REVISION HISTORY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.1 Publication of these Policies and Procedures		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	
None			

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.2 Privacy Document Archives		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 All Privacy and Security related documentation shall be stored on AIM's business network in a folder structure entitled "**Privacy & Security Documentation**" at the top level. This is referred to as the *privacy document archives*.

1.02 The document archives shall contain:

1. Privacy Code
2. Privacy & Security Policies and Procedures
3. Privacy Governance and Accountability Framework
4. Privacy Impact Assessments
5. Threat Risk Analyses
6. Staff Confidentiality Agreement Templates
7. Template of Privacy Notice at Termination of Employment or Contract
8. Copies of Staff Confidentiality Agreements
9. Privacy Training Documents (slide shows & handouts)
10. Log of Privacy Training Sessions and Attendance
11. Log of Data Holdings
    a. Description of Holdings
    b. Statements of Purpose
    c. Statements of Permitted Use
    d. Statements of Retention
12. Log of Authorized Personnel
13. Log of Accounts Having Access to PHI
14. Research Agreements
15. Log of Individual Requests to Access PHI
16. Data Sharing Agreements
    a. Template Data Sharing Agreements
    b. Log of Data Sharing Agreements
    c. Copies of Data Sharing Agreements
17. Third Party Service Agreements
    a. Template Third Party Service Agreements
    b. Log of Third Party Service Agreements
    c. Copies of Third Party Service Agreements
18. Log of Privacy Audits

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.2 Privacy Document Archives		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

19. Log of Privacy Breaches
20. Log of Privacy Complaints
21. Log of Individuals Having Access to Premises
22. Datacenter Entry/Exit Logs
23. Log of Security Breaches
24. Log of Security Audits
25. Log of PHI Transfers
26. Information Access Logs
27. Consolidated Log of Recommendations
28. Corporate Risk Register
29. Disaster Recovery Plan

2 PURPOSE

2.01 To provide a single point of access to Privacy & Security related documentation and to facilitate maintaining one published and approved version of the documentation.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that the privacy related documentation is stored in the appropriate network location and is complete and up-to-date.

5 DEFINITIONS

5.01 *Privacy Document Archives* refers to the network location/folder (on AIM's business network) under which the above listed documentation is stored.

6 REFERENCES and related POLICIES & PROCEDURES

None

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.3 Access to Privacy & Security Documentation		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 All staff shall be permitted to access the privacy document archives in read-only non-editable mode.

1.02 Designated staff shall have write-access to specific documents (such as logs) so that such documents may be kept up-to-date in the course of on-going operations.

2 PURPOSE

2.01 To provide staff with ready access to privacy policies and procedures and for designated individuals to be able to make updates to related documentation as required.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that document access rights and restrictions are properly configured and maintained in the privacy document archives.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.2 Privacy Document Archives

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.4 Employee/Contractee Confidentiality Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 All employees, and those contractees who may reasonably be expected to work with personal health information, shall execute a signed and witnessed **Personal Health Information Confidentiality and Non-Disclosure Agreement** describing the individual's obligations and responsibilities regarding the protection of personal health information.

1.02 **Personal Health Information Confidentiality and Non-Disclosure Agreements** shall be executed before the start of employment or contract and are in effect for the duration of employment or contract.

1.03 Should the standard **Personal Health Information Confidentiality and Non-Disclosure Agreement** be amended, all individuals having a previous agreement in effect shall be required to re-execute the new amended agreement.

2 PURPOSE

2.01 To ensure that staff formally agree to fulfill their personal obligations and responsibilities regarding the protection of personal health information and understand the potential ramifications and remedies in case of a breach of privacy or security.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that all current employees and/or contractees have an executed Personal Health Information Confidentiality and Non-Disclosure Agreement in effect.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.5 Template Confidentiality Agreements

PS 3.6 Executing Confidentiality Agreements

7 PROCEDURE

7.01 None

8 REVISION HISTORY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.4 Employee/Contractee Confidentiality Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	
None			

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.5 Template Confidentiality Agreements		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A template **Personal Health Information Confidentiality and Non-Disclosure Agreement** shall be maintained for employees and contractees.

1.02 The template agreement shall be readily available in the privacy document archives.

2 PURPOSE

2.01 To facilitate executing consistent agreements between employees and contractees regarding the protection of personal health information and that such agreements contain terms and conditions that align with prevailing legislation and regulations.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that Personal Health Information Confidentiality and Non-Disclosure Agreement templates are maintained current and available for use.

4.02 It is the responsibility of the President of Inscyte and the CEO of AIM Inc. to review and approve of template confidentiality agreements.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.4 Employee/Contractee Confidentiality Agreements

PS 3.6 Executing Confidentiality Agreements

PS 3.2 Privacy Document Archives

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.6 Executing Confidentiality Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 All employees of Inscyte and its agent AIM shall sign and execute a witnessed **Personal Health Information Confidentiality and Non-Disclosure Agreement** as a condition of employment and the agreement shall remain in effect as long as the individual is employed.

1.03 Prospective contractees of Inscyte or AIM who might be expected to work with personal health information shall also sign and execute a witnessed **Personal Health Information Confidentiality and Non-Disclosure Agreement** as a condition of the contract and the agreement shall remain in effect for the term of the contract.

1.04 In the event that the standard **Personal Health Information Confidentiality and Non-Disclosure Agreement** is amended, all individuals having such an agreement in effect shall be required to re-execute the new amended agreement.

1.05 Any individual who is required to, but refuses to sign the **Personal Health Information Confidentiality and Non-Disclosure Agreement** shall be denied employment or contract.

2 PURPOSE

2.01 To ensure that staff formally agree to fulfill their personal obligations and responsibilities regarding the protection of personal health information and to explicitly state the potential ramifications and remedies in case of breach.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that all staff execute Personal Health Information Confidentiality and Non-Disclosure Agreements prior to starting employment or contract services.

5 DEFINITIONS

5.01 An employee is a salaried individual for whom the company makes statutory deductions (income tax and other levies) from gross pay.

5.02 A contractee is an individual to whom Inscyte or AIM pays an agreed upon fee for service without any statutory deductions.

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.4 Employee/Contractee Confidentiality Agreements

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.6 Executing Confidentiality Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 3.5 Template Confidentiality Agreements

PS 3.2 Privacy Document Archives

7 PROCEDURE

7.01 Obtain a blank copy of the standard Personal Health Information Confidentiality and Non-Disclosure Agreement from AIM's business network. A template agreement can also be obtained from the Privacy Officer, Office Administrator or the Security Officer.

7.02 When presenting an individual with an Offer for Employment, the offer package must include the standard Personal Health Information Confidentiality and Non-Disclosure Agreement. The person making the offer must explicitly identify the requirement for executing this agreement.

7.03 When presenting an individual with Contract, the offer package should include the standard Personal Health Information Confidentiality and Non-Disclosure Agreement if it is reasonably expected that the individual will come into contact with PHI. If so, the person making the offer must explicitly identify the requirement for executing this agreement.

7.04 Have the individual sign and date the agreement in the presence of an employee. An employee should act as the witness whenever possible.

7.05 File the original signed/witnessed copy with personnel records.

7.06 Provide a copy of the original to individual for his/her retention.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.7 Privacy & Security Awareness Training		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 All employees shall undergo privacy awareness training on a regular basis.

1.02 Privacy awareness training sessions shall be conducted on a quarterly basis, typically coinciding with AIM's quarterly meetings.

1.03 Employee attendance at each privacy awareness training sessions shall be recorded with the individual's full name, date and signature.

1.04 A Log of Privacy Awareness Training Sessions shall be maintained listing the date of each session, the moderator/instructor's name, and a summary of the training session.

1.05 New hires shall be provided with one-on-one training as soon as is practical after the start of employment, but in any event, not later than three (3) months, being the probationary period.

2 PURPOSE

2.01 To promote on-going awareness of privacy and security issues and to communicate changes to prevailing legislation, regulations and/or best practices, and any recent amendments to the Privacy & Security Policies and Procedures.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to arrange for and ensure that privacy awareness training is provided to all employees at the time of hiring and on a regular basis thereafter.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.8 Maintaining Privacy Training Logs

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.8 Maintaining Privacy Training Logs		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A permanent record of Privacy Awareness Training sessions and employee attendance at these sessions shall be maintained.

2 PURPOSE

2.01 To provide evidence that regular privacy awareness training is conducted and that each attending individual has attested (by way of signature) that he/she has participated in the training.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that Privacy Training Logs are maintained complete and up-to-date.

5 DEFINITIONS

5.01 AIM's Privacy Training Log consists of a spreadsheet that lists all occurrences of privacy training sessions listing:

1) Session date
2) Session location
3) Moderator/Instructor's name
4) Session summary (topics covered, slide show, case studies etc.)

And:
A corresponding signed attendance list consisting of each attendee's full name and hand-written signature.

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.7 Privacy & Security Awareness Training

PS 3.2 Privacy Document Archives

7 PROCEDURE

7.01 Prior to each Privacy Awareness Session obtain a blank attendance form from the privacy documentation archives.

7.02 Ensure each person attending the session signs the attendance form prior to closing the session.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.8 Maintaining Privacy Training Logs		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.03 As soon as is practical following the session, amend the Privacy Training Log spreadsheet by adding information about the recently held session.

7.04 Scan an image of the attendance sheet and convert it to a non-editable file format.

7.05 Store the scanned image of the attendance sheet in the privacy documentation archives, section: Log of Privacy Training Sessions and Attendance.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.9 Monitoring Compliance with Policies and Procedures		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Compliance with Privacy & Security Policies and Procedures shall be monitored by conducting regular reviews of:

a) Privacy Logs to ascertain completeness and accuracy of entries
b) Computer servers, workstations and laptops to determine if personal health information is being stored inappropriately
c) Physical premises to ascertain if personal health information on portable media or in printed form is being handled/stored appropriately
d) Privacy document archives to ascertain completeness and currency of privacy documentation

1.02 The above mentioned reviews shall be carried out on a quarterly basis.

2 PURPOSE

2.01 To ensure that privacy policies and procedures are being followed.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that monitoring activities are conducted. The Privacy Officer may delegate this work to designated staff.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

None

7 PROCEDURE

7.01 Once per month, select an employee's computer at random and scan the computer for the presence of personal health information. If personal health information is found determine if this is a breach of privacy and proceed according to policy PS 11.3 Actions Following a Breach of Privacy

7.02 Once per quarter, review all privacy logs to determine if all required entries have been made. If required entries are missing correct the logs and speak with related personnel to remind them about the importance of maintaining accurate privacy logs.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.9 Monitoring Compliance with Policies and Procedures		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.03 Review document archives once per year coincident with the regular review of privacy and security policies and procedures to ensure that all privacy documentation is up-to-date and accounted for. Refer to policy PS 3.2 Privacy Document Archives for a list of documentation required.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.10 Corrective Action for Non-Compliance		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 In the event of non-compliance with Privacy & Security Policies and Procedures, corrective action shall be taken to remedy the non-compliance.

1.02 The nature of the corrective action shall be determined by the CEO taking into account the circumstances surrounding the non-compliance and the severity and consequences of the non-compliance.

1.03 If the non-compliance results in a breach of privacy, containment of the breach shall be the priority.

1.04 If the non-compliance results in a breach of security, repair of the breach shall be the priority.

1.05 Intentional non-compliance for the purpose of perpetrating a breach of privacy or security will result in termination of employment or contract and could incur other legal remedies available to the parties affected by the breach.

2 PURPOSE

2.01 This statement of corrective action is intended to reinforce the importance of the Privacy & Security Policies and Procedures.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is each employee's responsibility to report circumstances of non-compliance with these Privacy & Security Policies and Procedures to the Privacy Officer.

4.02 It is the responsibility of the Privacy Officer to inform the CEO of the non-compliance and to take appropriate corrective action to remedy the non-compliance.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

None

7 PROCEDURE

7.01 None

8 REVISION HISTORY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.10 Corrective Action for Non-Compliance		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	
None			

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.11 Actions at Termination of Employment or Contract		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 The following actions shall be taken upon termination of an individual's employment or contract:

a) Provide the individual with a letter of termination that expressly states that he/she must surrender any and all personal health information upon termination and that such information cannot be taken away from the business premises.
b) Obtain any keys issued to the individual.
c) Obtain any pass cards issued to the individual.
d) De-activate the individual's numeric lock passwords.
e) De-activate the individual's network access account(s).
f) De-activate the individual's application access account(s).
g) Check the individual's computer(s) for the presence of PHI.
h) Either archive or delete any PHI found on the individual's computer(s).
i) 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.

2 PURPOSE

2.01 To ensure that upon termination of employment individuals do not remove personal health information from the business premises and that any personal health information that the individual may have been working with is archived in secure storage (if needed) or destroyed.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that actions at the termination of an individual's employment or contract are fulfilled. The Privacy Officer may delegate the work to designated staff.

5 DEFINITIONS

5.01 See definition of personal health information in: PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	3 Implementation of Policies and Procedures		
PS 3.11 Actions at Termination of Employment or Contract		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 3.2 Privacy Document Archives

PS 5.2 Maintaining a Log of Authorized Personnel

PS 12.7 Log of Individuals Having Access to Premises

PS 12.8 Recovery of Keys, Pass Cards and Access Codes at Termination

PS 14.9 Log of Accounts Having Access to PHI

PS 14.10 Decommissioning of Accounts upon Termination

7 PROCEDURE

7.01 Obtain the current template Letter of Privacy Notice at Termination from the privacy document archives. Prepare the letter for the individual.

7.02 Have the individual read and sign the letter. Make a copy. File the copy with employee records.

7.03 Obtain keys and pass cards from the individual. Update the Log of Individuals Having Access to Premises noting the date and the name of the person who recovered the keys and pass cards.

7.04 Notify the technical services department to decommission the individual's computer system and application access accounts.

7.05 Update the Log of Accounts Having Access to PHI noting the date and the name of the person who de-activated the accounts.

7.06 Update the Log of Authorized Personnel to indicate the termination of employment and authorization to access/use PHI.

7.07 Technical services personnel must recover the individual's computer(s) and remove/archive any PHI found on the computer(s).

7.08 Inspect the individual's physical workspace and archive or destroy any PHI found in printed or on portable media.

8 REVISION HISTORY

None

4 Collection of Personal Health Information

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.1 Limits on the Collection of PHI		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal health information shall not be collected unless the collection of the information is permitted by the Act and its regulations.

1.02 The collection of personal health information shall be limited to the minimum amount and type of information that is necessary to fulfill the intended use of the information, and will not be collected if other information will serve the purpose.

1.03 No personal health information shall be collected in the absence of an identified requirement and approved purpose, permitted use, secure retention, and disposal/return mechanism which shall be documented in the statements of purpose, permitted use, and retention for each data holding.

1.04 Collection of personal health information requires a legally binding **Data Sharing Agreement** to be executed between Inscyte and the custodian/provider of the information prior to the collection of the information.

2 PURPOSE

2.01 To ensure that all personal health information is collected for a prescribed and approved purpose and limited to the amount and type of information required to support the intended use.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and AIM Inc. as its Agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the President of Inscyte to review and approve of the collection of personal health information from custodians/providers and to execute Data Sharing Agreements with these entities prior to the collection of personal health information.

4.02 It is the responsibility of the Privacy Officer to enforce limits on the collection of personal health information in accordance with this policy.

4.03 It is the responsibility of each and every individual to report a breach of this policy in accordance with policy and procedure PS 11.2 Reporting a Breach of Privacy.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.1 Limits on the Collection of PHI		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 4.7 Maintaining Logs of Data Holdings

PS 4.8 Maintaining Statements of Purpose

PS 4.9 Maintaining Statements of Permitted Use

PS 4.10 Maintaining Statements of Retention

PS 4.11 Unsolicited Receipt of PHI

PS 7.1 Requirement for Data Sharing Agreements

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.2 Collection of PHI – Paper Records		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 If personal health information is to be collected in paper-based format (clinical report forms, letters, lab reports, etc.) the following precautions shall be taken during the collection process:

(a) The paper-based records shall be enclosed in a sealed envelope or box
(b) The packages shall identify the individual recipient and sender of the information
(c) The package shall identify the date when the records were sealed
(d) The package should be labeled to clearly describe that it contains PHI and the nature of the content. For example: "PHI: Inscyte CytoBase Lab Results for Manual Correction".

1.02 Paper-based records may not be transported by federal post. Paper-based records shall be transported via commercial courier or by the designated staff of either the sender or recipient.

1.03 The package of paper-based records should not be left unattended and publicly visible during the collection process.

2 PURPOSE

2.01 To safeguard personal health information from inadvertent disclosure or loss during the collection process.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure appropriate safeguards are implemented during the collection of personal health information in paper-based format.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 4.3 Collection of PHI – Portable Media

PS 4.4 Collection of PHI – Mobile Devices

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.2 Collection of PHI – Paper Records		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 4.5 Collection of PHI – Email

PS 4.6 Collection of PHI – Network Transfer

PS 13.2 Storage of PHI – Paper Records

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.3 Collection of PHI – Portable Media		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 If personal health information is to be collected using portable media (see definition below) the following precautions shall be taken during the collection process:

(a) The files on the portable media that contain personal health information shall be encrypted and password protected, and/or
(b) The portable memory device itself shall be password protected.
(c) The portable media should be labeled to clearly describe that it contains PHI and the nature of the content. For example: "PHI: Inscyte CytoBase Lab Results for Manual Correction".

1.02 Portable media shall not be transported by federal post. Portable media shall be transported via commercial courier or by the designated staff of either the sender or recipient.

1.03 Portable media containing PHI should not be left unattended and publicly visible during the collection process.

2 PURPOSE

2.01 To safeguard personal health information from inadvertent disclosure or loss during the collection process.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure appropriate safeguards are implemented during the collection of personal health information using portable media.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

5.02 **Portable Media** means diskettes, tapes, CDs, DVDs, USB keys and other portable information storage media.

6 REFERENCES and related POLICIES & PROCEDURES

PS 4.2 Collection of PHI – Paper Records

PS 4.4 Collection of PHI – Mobile Devices

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.3 Collection of PHI – Portable Media		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 4.5 Collection of PHI – Email

PS 4.6 Collection of PHI – Network Transfer

PS 13.3 Storage of PHI – Portable Media

PS 14.5 Requirements for Access Accounts

PS 14.6 Requirements for Passwords

7 PROCEDURE

7.01 To encrypt and password protect a file (or set of files) it is permissible to use a commercial software tool such as PK-Zip or WinZip.

7.02 The password used to lock the file(s) must not be noted or contained with the portable media itself. The password should be communicated to the receiver by telephone or by an email message.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.4 Collection of PHI – Mobile Devices		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal health information shall not be collected using mobile devices.

2 PURPOSE

2.01 To safeguard personal health information from inadvertent disclosure or loss during the collection process.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its Agent.

4 RESPONSIBILITY

4.01 It is the responsibility of every individual to ensure that no personal health information is collected using mobile devices.

4.02 It is the responsibility of the Security Officer to periodically audit the use of mobile devices to monitor compliance with this policy.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

5.02 **Mobile Devices** means portable computing devices that can be used alone to store, retrieve, and manipulate data, such as laptops, notebooks, tablets, PDAs, and smart phones.

6 REFERENCES and related POLICIES & PROCEDURES

PS 4.2 Collection of PHI – Paper Records

PS 4.3 Collection of PHI – Portable Media

PS 4.5 Collection of PHI – Email

PS 4.6 Collection of PHI – Network Transfer

PS 13.4 Storage of PHI – Mobile Devices

PS 13.15 Disposal of PHI – Files/Database Systems

PS 14.5 Requirements for Access Accounts

PS 14.6 Requirements for Passwords

7 PROCEDURE

7.01 None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.4 Collection of PHI – Mobile Devices		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.5 Collection of PHI – Email		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal health information should not be collected using email unless the personal health information is contained in a file attachment and the file is encrypted and password protected.

1.02 The password to unlock an encrypted file attachment shall not be communicated to the recipient using email. It should be communicated to the recipient personally by telephone allowing the sender to verify the recipient's identity.

1.03 Any personal health information received via email or an email attachment should be saved to a location on a server that is part of the secure PHI network and the email message should be deleted from the email client and the email server forthwith.

2 PURPOSE

2.01 To safeguard personal health information from inadvertent disclosure, theft or loss during the collection process.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure appropriate safeguards (tools) are implemented during the collection of personal health information via email.

4.02 It is the responsibility of every individual to ensure that collection of PHI using email complies with this policy but, in any event, is avoided whenever possible.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 4.2 Collection of PHI – Paper Records

PS 4.3 Collection of PHI – Portable Media

PS 4.4 Collection of PHI – Mobile Devices

PS 4.6 Collection of PHI – Network Transfer

PS 13.5 Storage of PHI – Email Archives

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.5 Collection of PHI – Email		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 13.15 Disposal of PHI – Files/Database Systems

PS 14.6 Requirements for Passwords

PS 14.1 Isolation of PHI Computers and Networks

7 PROCEDURE

7.01 To encrypt and password protect a file (or set of files) it is permissible to use a commercial software tool such as PK-Zip or WinZip.

7.02 The password used to lock the file(s) must not be noted or contained within the email message. The password should be communicated to the receiver by telephone or other means.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.6 Collection of PHI – Network Transfer		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 If personal health information is to be collected using data transfer over a computer network the following precautions shall be taken during the collection process:

(a) The network connection between sending and receiving systems shall be encrypted using a self-managed or third-party public key infrastructure (PKI) mechanism.
(b) Access to the network shall require authentication of a unique account name and password combination (user login).

1.02 In addition, when possible, individual files (or messages) being transferred should also be encrypted even if the network itself is encrypted (i.e. use double encryption).

2 PURPOSE

2.01 To safeguard personal health information from inadvertent disclosure or loss during the collection process.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure appropriate safeguards are implemented during the collection of personal health information using network transfer.

4.02 It is the responsibility of every individual handling PHI to ensure that network transfers of PHI comply with this policy.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 4.2 Collection of PHI – Paper Records

PS 4.3 Collection of PHI – Portable Media

PS 4.4 Collection of PHI – Mobile Devices

PS 4.5 Collection of PHI – Email

7 PROCEDURE

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.6 Collection of PHI – Network Transfer		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.01 Network transfer of personal health information should be used when the collection process is on-going or repetitive.

7.02 Acceptable encryption strength is 1024 bits or higher.

7.03 If collection of PHI is performed using a network application (such as a web application) use a third-party server security certificate on the application server to encrypt and secure the network connection (e.g. VeriSign)

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.7 Maintaining Logs of Data Holdings		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte shall maintain a an up-to-date list and description of the data holdings of personal health information that it maintains.

2 PURPOSE

2.01 In accordance with Act, holdings of personal health information shall be clearly identified and documented with respect to:

(a) Description of the holding
(b) The data content
(c) The method of collection
(d) The storage medium and physical location
(e) Safeguards
(f) Access restrictions
(g) Statement of Purpose
(h) Statement of Permitted use of the data
(i) Statement of Retention of the data

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that an up-to-date log of data holdings is maintained and amended as appropriate.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 4.8 Maintaining Statements of Purpose

PS 4.9 Maintaining Statements of Permitted Use

PS 4.10 Maintaining Statements of Retention

PS 3.2 Privacy Document Archives

7 PROCEDURE

7.01 The log of data holdings is to be maintained and stored in the Privacy Document Archives: Section 11 – Log of Data Holdings

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.7 Maintaining Logs of Data Holdings		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.8 Maintaining Statements of Purpose		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte shall maintain up-to-date **Statements of Purpose** for each of the data holdings of personal health information that it maintains.

1.02 In creating or amending statements of purpose, the source(s) of the personal health information shall be consulted and permitted to review the statements of purpose.

1.03 Statement of Purpose shall be approved by the President of Inscyte.

1.04 Statements of Purpose shall be made available to the source(s) (i.e. healthcare custodians) of the personal health information. In particular, this includes the medical laboratories providing test results to CytoBase.

1.05 Statement of Purpose shall be reviewed for accuracy and applicability in conjunction with the annual review of privacy policies and procedures.

2 PURPOSE

2.01 In accordance with Act, holdings of personal health information shall have a documented **Statement of Purpose** that describes:

(a) The purpose of the holding
(b) Description of the personal health information contained in the holding
(c) The need for collecting the data in relation to the purpose
(d) The source(s) of the data

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that up-to-date statements of purpose are maintained and amended as appropriate for each holding of personal health information and for conducting reviews of statements of purpose.

4.02 It is the responsibility of the President of Inscyte to approve new or amen ended statements of purpose.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 4.7 Maintaining Logs of Data Holdings

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.8 Maintaining Statements of Purpose		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 4.9 Maintaining Statements of Permitted Use

PS 4.10 Maintaining Statements of Retention

PS 3.2 Privacy Document Archives

7 PROCEDURE

7.01 Statements of Purpose are to be maintained and stored in the Privacy Document Archives: Section 11 – Log of Data Holdings, sub-section Statements of Purpose.

7.02 When creating a new Statement of Purpose, use the document template stored at that location.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.9 Maintaining Statements of Permitted Use		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte shall maintain up-to-date **Statements of Permitted Use** for each of the data holdings of personal health information that it maintains.

1.02 Inscyte and its agent(s) may only access and use a data holdings of personal health information in accordance with the constraints described in the **Statement of Permitted Use** for each holding.

2 PURPOSE

2.01 In accordance with the Act, holdings of personal health information shall have a documented Statement of Permitted Use that describes:

(a) Who may access and use the data
(b) The type of work functions that require access to the data
(c) Limits on the use of the data

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that up-to-date Statements of Permitted Use are maintained and amended as appropriate for each holding of personal health information.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 4.7 Maintaining Logs of Data Holdings

PS 4.8 Maintaining Statements of Purpose

PS 4.10 Maintaining Statements of Retention

PS 3.2 Privacy Document Archives

7 PROCEDURE

7.01 Statements of Permitted Use are to be maintained and stored in the Privacy Document Archives: Section 11 – Log of Data Holdings, sub-section Statements of Permitted Use.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.9 Maintaining Statements of Permitted Use		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.02 When creating a new Statement of Permitted Use, use the document template stored at that location.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.10 Maintaining Statements of Retention		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte shall maintain up-to-date **Statements of Retention** for each of the data holdings of personal health information that it maintains.

1.04 Inscyte shall retain and dispose of personal health information in accordance with the provisions of the **Statement of Retention** for each of the data holdings of personal health information that it maintains.

2 PURPOSE

2.01 In accordance with the Act, holdings of personal health information shall have a documented Statement of Retention that describes:

(a) The retention period for the data (or sub-sets of the data)
(b) The method of secure disposal (or return) to be used when the retention period expires
(c) Who may dispose of the data
(d) Audit and tracking of the data from collection through the end of the retention period

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that up-to-date Statements of Retention are maintained and amended as appropriate for each holding of personal health information.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 4.7 Maintaining Logs of Data Holdings

PS 4.8 Maintaining Statements of Purpose

PS 4.9 Maintaining Statements of Permitted Use

PS 3.2 Privacy Document Archives

7 PROCEDURE

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.10 Maintaining Statements of Retention		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.01 Statements of Retention are to be maintained and stored in the Privacy Document Archive, section: Log of Data Holdings, sub-section Statements of Retention.

7.02 When creating a new Statement of Retention, use the document template stored at that location.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.11 Unsolicited Receipt of PHI		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Upon receipt of unsolicited personal health information, the sender of the information shall be notified about the breach of privacy and the nature of the disclosure.

1.02 The unsolicited personal health information shall be promptly destroyed, returned, or de-identified as per the instructions of the custodian/provider of the information.

1.03 A breach of privacy shall be reported to the Privacy Officer as per policy and procedure PS 11.2 Reporting a Breach of Privacy.

2 PURPOSE

2.01 To ensure that personal health information disclosed to Inscyte and/or its agent(s) accidentally or in error is contained and that the sender of the information is alerted to the breach of privacy.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of each individual to identify and respond to the unsolicited receipt of personal health information and report the breach to the Privacy Officer.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

5.02 “Unsolicited personal health information” is personal health information that is received in error and/or outside of Data Sharing Agreement between the custodian/provider of the information and Inscyte Corporation, or its agent(s).

6 REFERENCES and related POLICIES & PROCEDURES

PS 11.1 Indentifying a Breach of Privacy

PS 11.2 Reporting a Breach of Privacy

PS 3.2 Privacy Document Archives

7 PROCEDURE

7.01 Upon receipt of unsolicited personal health information, store the information on a secure network location or in secured offices.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	4 Collection of Personal Health Information		
PS 4.11 Unsolicited Receipt of PHI		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.02 Contact the sender (preferably by telephone) and explain that you have received "patient identified health information in error" and that this is a breach of privacy.

7.03 Ask the sender if he/she prefers AIM to promptly destroy the information, return it (if on paper or portable media/device) or de-identify it. One of these options must be exercised.

7.04 If the sender cannot be contacted with a reasonable time frame, destroy the information and notify the sender that the information has been destroyed.

7.05 Log the breach in the Privacy Document Archives: Section 22 – Log of Privacy Breaches.

7.06 Prepare a privacy breach report and forward it to the Privacy Officer for review.

8 REVISION HISTORY

None

5 Use of Personal Health Information

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	5 Use of Personal Health Information		
PS 5.1 Limiting Access to and Use of PHI		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal health information shall not be used unless the use of the information is permitted by the Act and its regulations.

1.02 Personal health information shall only be used in accordance with the **Statement of Permitted Use** for each data holding.

1.05 Access to, and use of personal health information by participating laboratories (or other organizations) shall require a legally binding **Data Sharing Agreement** to be executed between Inscyte and each participating laboratory/organization.

1.06 Access to personal health information shall be limited based on the "need to know" principle to a only those individuals who are required to work with the information.

1.07 The scope of personal information used in carrying out the work shall be limited to the least identifiable information and minimum amount of information required to complete the work.

1.08 Access to, and use of holdings of personal health information by individuals shall require prior approval by the Privacy Officer.

1.09 For all other purposes and circumstances, personal health information shall be de-identified and/or aggregated.

2 PURPOSE

2.01 To minimize the potential for unauthorized use and/or disclosure of personal health information.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that limits on access and use of personal health information are in effect.

4.02 It is the responsibility of the Privacy Officer to approve of access to holdings of personal health information by individuals.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	5 Use of Personal Health Information		
PS 5.1 Limiting Access to and Use of PHI		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 4.9 Maintaining Statements of Permitted Use

PS 9.2 De-Identification of PHI – Paper Records

PS 9.3 De-Identification of PHI – Digital Records

PS 9.4 Limits on Aggregation of Data (Statistics)

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	5 Use of Personal Health Information		
PS 5.2 Maintaining a Log of Authorized Personnel		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A permanent record shall be maintained of all employees and contractees of Inscyte and/or its agent AIM Inc. who have been authorized to access and use personal health information.

1.02 The **Log of Authorized Personnel** shall contain the following minimum information:

(a) The full name of the individual authorized to access/use a CytoBase data holding
(b) The name of the data holding to which access was granted
(c) The date of authorization
(d) The reason for granting the access
(e) A description of the level of access or constraints (if any)
(f) The date of revocation
(g) Reason for revocation

1.03 The **Log of Authorized Personnel** shall be updated when:

(a) An individual is authorized to access/use a PHI data holding
(b) An individual's rights to access a PHI data holding is revoked
(c) An individual ceases to be employed or contracted

2 PURPOSE

2.01 To maintain a perpetual record of individuals who at one time or another had access to data holdings of personal health information and the duration of those access rights.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that the Log of Authorized Personnel is maintained complete, accurate and up-to-date.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.2 Privacy Document Archives

PS 14.9 Log of Accounts Having Access to PHI

7 PROCEDURE

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	5 Use of Personal Health Information		
PS 5.2 Maintaining a Log of Authorized Personnel		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.01 None

8 REVISION HISTORY

None

6 Disclosure of Personal Health Information

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	6 Disclosure of Personal Health Information		
PS 6.1 Limits on Disclosure of PHI		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal health information shall be disclosed only where disclosure of the personal health information is permitted or required by law.

1.02 Disclosure of personal health information shall be reviewed and approved of by the Privacy Officer prior to the disclosure taking place.

1.03 In general, aggregate information with fewer than five (5) observations per aggregation is not to be disclosed.

2 PURPOSE

2.01 To limit the disclosure and use of personal health information in CytoBase to the purposes for which it was collected and those permitted under Ontario's *Personal Health Information Protection Act, 2004*., and its regulations.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 The Privacy Officer shall ensure that up-to-date documentation is maintained describing each individual and/or organization to which Inscyte Corporation discloses or has disclosed personal health information, the purpose of the disclosure and the statutory authority for such disclosure.

4.01 The Privacy Officer shall be responsible for determining the authority under which personal health information may be disclosed to individuals and/or organizations and for approving the disclosure.

4.02 In cases where disclosure of personal health information is required by law, the Privacy Officer shall be responsible for obtaining a copy of the legislation, subpoena or summons giving effect to the legal requirement for the disclosure.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

Inscyte Corporation Privacy Code – Rev 2.0 August 2008

PS 6.2 Disclosure of PHI for Purposes other than Research

PS 6.3 Disclosure of PHI for Research Purposes

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	6 Disclosure of Personal Health Information		
PS 6.1 Limits on Disclosure of PHI		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 6.4 Request by an Individual to Access his/her PHI

PS 9.4 Limits on Aggregation of Data (Statistics)

7 PROCEDURE

7.01 Prior to disclosure of personal health information, meet with the Privacy Officer or designated delegate to review the authority under which the disclosure can be made and complete the required documentation pertaining to the disclosure.

7.02 Prior to the disclosure of any aggregated information, the Privacy Officer shall review the information to assess the risk of 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 the purpose of the disclosure. If the risk is deemed inappropriate the information shall not be disclosed. In assessing the risk of inadvertent disclosure, the Privacy Officer shall have regard to section 4(2) of Ontario's *Personal Health Information Protection Act, 2004*, 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.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	6 Disclosure of Personal Health Information		
PS 6.2 Disclosure of PHI for Purposes other than Research		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal health information may be disclosed to authorized parties for the general purpose of improving patient care and maintaining system operations subject to the provisions of policy PS 6.1 Limits on Disclosure of PHI.

1.02 Disclosure of personal health information shall require a legally binding **Data Sharing Agreement** to be executed between Inscyte Corporation and the individual or organization to whom the personal health information is to be disclosed before the disclosure can take place.

1.03 Disclosure of personal health information to an individual in the employ of Inscyte Corporation or its agent(s) requires a contractual **Confidentiality and Non-Disclosure Agreement** to be executed between the employer and each designated individual before the disclosure can take place.

1.04 Disclosure of personal health information shall be reviewed and approved of by the Privacy Officer prior to the disclosure taking place.

2 PURPOSE

2.01 To limit the disclosure and use of personal health information to the purposes for which it was collected and those permitted under Ontario's *Personal Health Information Protection Act, 2004*., and its regulations.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that disclosure of personal health information for purposes other than research is conducted in accordance with these policies and procedures.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

Inscyte Corporation Privacy Code – Rev 2.0 August 2008

PS 3.6 Executing Confidentiality Agreements

PS 6.1 Limits on Disclosure of PHI

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	6 Disclosure of Personal Health Information		
PS 6.2 Disclosure of PHI for Purposes other than Research		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 6.3 Disclosure of PHI for Research Purposes

PS 6.4 Request by an Individual to Access his/her PHI

PS 7.1 Requirement for Data Sharing Agreements

PS 9.4 Limits on Aggregation of Data (Statistics)

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	6 Disclosure of Personal Health Information		
PS 6.3 Disclosure of PHI for Research Purposes		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal health information shall not be disclosed for the purpose of conducting research on individuals and/or groups of individuals.

1.02 Disclosure of de-identified information is permitted (i.e. information that does not constitute personal health information) for purposes of aggregation and analysis.

1.03 Aggregate information with fewer than five (5) observations per aggregation is not to be disclosed.

2 PURPOSE

2.01 To limit the disclosure and use of personal health information to the purposes for which it was collected and those permitted under Ontario's *Personal Health Information Protection Act, 2004*., and its regulations.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that disclosure of personal health information for research purposes is restricted in accordance with these policies and procedures.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

Inscyte Corporation Privacy Code – Rev 2.0 August 2008

PS 6.1 Limits on Disclosure of PHI

PS 6.2 Disclosure of PHI for Purposes other than Research

PS 6.4 Request by an Individual to Access his/her PHI

PS 9.4 Limits on Aggregation of Data (Statistics)

7 PROCEDURE

7.01 Prior to the disclosure of any aggregated information, the Privacy Officer shall review the information to assess the risk of 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 the purpose of the disclosure. If the

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	6 Disclosure of Personal Health Information		
PS 6.3 Disclosure of PHI for Research Purposes		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

risk is deemed inappropriate the information shall not be disclosed. In assessing the risk of inadvertent disclosure, the Privacy Officer shall have regard to section 4(2) of Ontario's *Personal Health Information Protection Act, 2004*, 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.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	6 Disclosure of Personal Health Information		
PS 6.4 Request by an Individual to Access his/her PHI		Effective:	Nov 1, 2011
		Pages:	4
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte Corporation will provide information to an individual or to an individual's legal substitute decision maker, about the existence, use, and disclosure of the personal health information held on that individual provided that:

(a) The individual submits a written request
(b) The individual provides acceptable proof of identity
(c) Inscyte Corporation is not legally prevented from providing the information
(d) The information is not subject to solicitor-client or litigation privilege

1.02 Should an individual inquire about the procedure for requesting information about the existence, use and disclosure of personal health information held on that individual, Inscyte Corporation will provide the individual with a copy of this policy/procedure.

1.03 Requests should be made in writing and submitted by fax or regular mail to:

Privacy Officer
Inscyte Corporation
2 Berkeley Street, Suite 403
Toronto, Ontario
M5A 2W3
Fax: (416) 594-2420

1.04 The request shall include:

(a) The full name of the individual that is the subject of the request
(b) The individual's Provincial health insurance number (but not the production of the Health Card)
(c) The individual's complete date of birth
(d) If the requester is a legal substitute decision maker for the individual that is the subject of the request, then also require:
    a. Full name of the requester
    b. Proof of legal status as the substitute decision maker for the individual
(e) The requester's current address of residence
(f) The requester's contact information (e.g. address, telephone, email)
(g) The date of the request
(h) The requester's signature
(i) One of the following to establish proof of identity of the requester:
    a. Certified copies of two pieces of photographic identification (e.g. driver's license, passport, professional ID), or

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	6 Disclosure of Personal Health Information		
PS 6.4 Request by an Individual to Access his/her PHI		Effective:	Nov 1, 2011
		Pages:	4
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

b. An affidavit from a notary public or lawyer that certifies that the requester is the individual they claim to be.

(j) Inscyte Corporation shall provide a pre-printed "Request for Individual Access to Personal Health Information" form in paper and electronic formats to guide individuals in the process of making a request.

1.05 Inscyte Corporation shall not provide or disclose laboratory test results to an individual, only the existence of such test results. Should the individual wish to challenge the existence or content of the test results, Inscyte will refer the individual to the appropriate healthcare custodian from whom the personal health information was originally received (e.g. member laboratories) for resolution of the challenge.

1.06 Inscyte Corporation may, at its sole discretion, charge a reasonable fee for processing a request to cover expenses associated with the retrieval, formatting, and delivery of the information. In this case, the amount shall be communicated to the requester before the request is processed. Inscyte Corporation may waive the fee at its discretion.

2 PURPOSE

2.01 The *Personal Health Information Protection Act, 2004* makes provision for an individual to gain access to his/her records and to challenge the accuracy of those records.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to review and approve all requests for individual access ensuring that acceptable proof of identity has been provided with each request.

4.02 It is the responsibility of the Privacy Officer to ensure that all requests are processed forthwith and logged.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

Inscyte Corporation Privacy Code – Rev 2.0 August 2008

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	6 Disclosure of Personal Health Information		
PS 6.4 Request by an Individual to Access his/her PHI		Effective:	Nov 1, 2011
		Pages:	4
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 6.1 Limits on Disclosure of PHI

PS 6.2 Disclosure of PHI for Purposes other than Research

PS 6.3 Disclosure of PHI for Research Purposes

7 PROCEDURE

7.01 Obtain a blank copy of the **Request for Individual Access to Personal Health Information** form from AIM's privacy documentation archives and provide the form (on paper or electronic copy) to the individual making the request with instructions on how to fill out the form.

7.02 The Privacy Officer shall review each request about the existence, use and disclosure of the personal health information held on that individual and ensure that acceptable proof of identity has been provided with the request.

7.03 The Privacy Officer, or delegate, shall respond to each request indicating to the requester the status of the request and any applicable fees. This may be communicated verbally, by electronic means, or by post.

7.04 Prepare a "Report of Personal Health Information" containing:

(a) The health insurance number, surname, and date of birth of the individual who is the subject of the request.
(b) The date the request was processed.
(c) The name of the operator who processed the request.
(d) The date of each test result on file for the individual and
(e) Information about the use and disclosure of the personal health information taken from the audit logs.

Store the report together with a scanned image of the request form in AIM's privacy documentation archives, section: Log of Individual Requests to Access PHI. These documents are to be retained in perpetuity.

7.05 The Report of Personal Health Information of the individual will only be made available to the requester in printed form. Disclosure by electronic means or digital media is prohibited.

7.06 The Report of Personal Health Information will be placed in an envelope labeled with the requester's full name and address and will include a copy of the original request and the proof of identity provided with the request. Until pick-up, this information shall be stored in a secure location.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	6 Disclosure of Personal Health Information		
PS 6.4 Request by an Individual to Access his/her PHI		Effective:	Nov 1, 2011
		Pages:	4
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.07 To obtain the Report of Personal Health Information, the requester must pick up the information in person from the offices of Inscyte Corporation or its agents.

7.08 The requester must bring the original versions of the proof of identification submitted with the request or affidavit.

7.09 Verify that the identification presented by the requester at pick up matches the identification provided with the original request. The Report of Personal Health Information may only be turned over to the requester if the identification information matches.

7.10 If the individual challenges the accuracy of the personal health information disclosed in the Report of Personal Health Information, the Privacy Officer shall refer the individual to the health information custodian who originally provided the information to Inscyte Corporation (e.g. member laboratories) for resolution.

8 REVISION HISTORY

None

7 Data Sharing Agreements

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	7 Data Sharing Agreements		
PS 7.1 Requirement for Data Sharing Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Prior to the collection, use, and/or disclose of personal health information with another party, a formal Data Sharing Agreement shall be executed between Inscyte Corporation and the other party subject to the minimum content requirements described in policy PS 7.2 Minimum Content of Data Sharing Agreements.

1.02 The parties to a Data Sharing Agreement shall be legally permitted to share personal health information under the provisions of the Personal Health Information Protection Act, 2004 Ontario, and any regulations to this Act. This effectively restricts data sharing to parties that are either healthcare custodians, prescribed persons, or prescribed entities.

1.03 Only the President of Inscyte may legally bind Inscyte Corporation to the terms and conditions of a Data Sharing Agreement.

2 PURPOSE

2.01 To specify the legal authority and the terms and conditions under which personal health information can be collected, used and disclosed with another party before the collection, use or disclosure can occur.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and AIM Inc. as its Agent.

3.02 This policy applies when CytoBase information is to be shared between healthcare custodians, prescribed persons, or prescribed entities regulated by the Personal Health Information Protection Act, 2004, Ontario.

4 RESPONSIBILITY

4.01 It is the responsibility of the President of Inscyte to ensure that Data Sharing Agreements have been executed between Inscyte Corporation and providers or receivers of personal health information before collection, use and disclosure of personal health information can take place.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 7.2 Minimum Content of Data Sharing Agreements

PS 7.3 Template Data Sharing Agreements

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	7 Data Sharing Agreements		
PS 7.1 Requirement for Data Sharing Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 7.4 Log of Data Sharing Agreements

7 PROCEDURE

7.01 To prepare a new Data Sharing Agreement, obtain a template Data Sharing Agreement from AIM's privacy document archives.

7.02 Prior to executing a Data Sharing Agreement, provide a copy to the Privacy Officer for review and approval.

7.03 Provide a final copy to the President of Inscyte for signature.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	7 Data Sharing Agreements		
PS 7.2 Minimum Content of Data Sharing Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 At a minimum, a Data Sharing Agreement shall contain the following information:

(a) Legal names of both parties
(b) Contact information for both parties
(c) Effective date of the agreement
(d) Termination or expiry date of the agreement
(e) The authority under which the data may be shared
(f) A detailed description of the personal health information to be shared
(g) Terms and conditions setting out:
    a. The method of collection (or linkage)
    b. The permitted use of the data
    c. The retention period for the data (by each party)
    d. Limits on disclosure of the data (for each party)
    e. Requirements for destruction or disposal of the data (for each party)

1.02 All Data Sharing Agreements shall explicitly identify Inscyte Corporation as a Prescribed Person under regulation 329/04 to the Personal Health Information Protection Act, 2004, Ontario (the Act).

1.03 All Data Sharing Agreements shall include a definition of personal health information as per the Act.

1.04 All Data Sharing Agreements shall attest to the fact that the parties to the agreement have in place privacy and security policies and procedures to safeguard personal health information in compliance with the requirements of the Act and its regulations.

2 PURPOSE

2.01 To ensure that Data Sharing Agreements include all relevant information so that both Inscyte Corporation and the other party understand the legal framework and terms and conditions under which personal health information will be collected, used or disclosed.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and AIM Inc. as its Agent.

3.02 This policy applies when CytoBase information is to be shared between healthcare custodians, prescribed persons, or prescribed entities regulated by the Personal Health Information Protection Act, 2004, Ontario.

4 RESPONSIBILITY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	7 Data Sharing Agreements		
PS 7.2 Minimum Content of Data Sharing Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

4.01 It is the responsibility of the Privacy Officer to ensure that Data Sharing Agreements contain the minimum required amount of information.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 7.1 Requirement for Data Sharing Agreements

PS 7.3 Template Data Sharing Agreements

PS 7.4 Log of Data Sharing Agreements

7 PROCEDURE

7.01 To prepare a new Data Sharing Agreement, obtain a template Data Sharing Agreement from AIM's privacy document archives.

7.02 Prior to executing a Data Sharing Agreement, provide a copy to the Privacy Officer for review and approval.

7.03 Provide a final copy to the President of Inscyte for signature.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	7 Data Sharing Agreements		
PS 7.3 Template Data Sharing Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A standard template Data Sharing Agreement shall be maintained in the privacy documentation archives.

1.02 The template Data Sharing Agreement shall be used to prepare new data sharing agreements.

1.03 The template Data Sharing Agreement shall be updated when:

(a) There is a requirement to change the minimum content of the agreement
(b) There is a change in prevailing legislation or regulations
(c) The Office of the Information and Privacy Commissioner requires a change

1.04 Each template agreement shall be identified with a unique revision number and date of issue.

1.05 Template Data Sharing Agreements shall be approved by the President of Inscyte prior to issue.

2 PURPOSE

2.01 To ensure that Data Sharing Agreements are consistent and include all relevant information so that both Inscyte Corporation and the other party understand the legal framework and terms and conditions under which personal health information will be collected, used and/or disclosed.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and AIM Inc. as its Agent.

3.02 This policy applies when CytoBase information is to be shared between healthcare custodians, prescribed persons, or prescribed entities regulated by the Personal Health Information Protection Act, 2004, Ontario.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that a current standard template Data Sharing Agreement is maintained in the privacy documentation archives and that this template agreement is used to prepare new data sharing agreements.

4.02 It is the responsibility of the President of Inscyte to review and approve of template data sharing agreements.

5 DEFINITIONS

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	7 Data Sharing Agreements		
PS 7.3 Template Data Sharing Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 7.1 Requirement for Data Sharing Agreements

PS 7.2 Minimum Content of Data Sharing Agreements

PS 7.4 Log of Data Sharing Agreements

7 PROCEDURE

7.01 To prepare a new or updated template Data Sharing Agreement, obtain the previous template (if any) from the privacy document archives or start a new template.

7.02 Make modifications to the new template and store it as a “draft” for approval.

7.03 Provide the draft template to the Privacy Officer for review.

7.04 Upon approval of the new template Data Sharing Agreement, increment its revision number, update the issue date, and mark the template as “Final”.

7.05 Store the template in the privacy documentation archives, section: Data Sharing Agreements.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	7 Data Sharing Agreements		
PS 7.4 Log of Data Sharing Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A log of Data Sharing Agreements shall be maintained containing:

(a) The name of the parties to the agreement
(b) The current status of the agreement (active, expired, etc.)
(c) The location where the signed agreement itself is stored
(d) The effective date of the agreement
(e) The termination/expiry date of the agreement
(f) A brief description of the agreement
(g) A brief description of the reason the agreement was terminated (if applicable)

1.02 The log of Data Sharing Agreements shall be updated when:

(a) A new Data Sharing Agreement is executed
(b) A Data Sharing Agreement expires
(c) A Data Sharing Agreement is terminated by either party

2 PURPOSE

2.01 To maintain a perpetual, complete and accurate record of data sharing agreements executed between Inscyte Corporation and third parties.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and AIM Inc. as its Agent.

3.02 This policy applies when CytoBase information is to be shared between healthcare custodians, prescribed persons, or prescribed entities regulated by the Personal Health Information Protection Act, 2004, Ontario.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that the log of Data Sharing Agreements is maintained current, complete and accurate. The Privacy Officer may delegate the updates of the log to designated staff.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 7.1 Requirement for Data Sharing Agreements

PS 7.2 Minimum Content of Data Sharing Agreements

PS 7.3 Template Data Sharing Agreements

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	7 Data Sharing Agreements		
PS 7.4 Log of Data Sharing Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7 PROCEDURE

7.01 To make a new entry in the log of Data Sharing Agreements or to update an entry, access the log file (Microsoft Excel File) in the privacy document archives, section: Data Sharing Agreements.

7.02 Update the file and save it.

8 REVISION HISTORY

None

8 Agreements with Third Party Service Providers

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	8 Agreements with Third Party Service Providers		
PS 8.1 Requirement for Third Party Service Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 In the event that a third party is required to provide services related to the operations of CytoBase, a formal Third Party Service Agreement shall be executed between Inscyte Corporation and the service provider before the services can be rendered and subject to the minimum content requirements specified in policy PS 8.2 Minimum Content of Third Party Service Agreements.

1.02 Only the President of Inscyte may legally bind Inscyte Corporation to the terms and conditions of a Third Party Service Agreement.

2 PURPOSE

2.01 To inform the service provider about the status of Inscyte Corporation as a Prescribed Person under regulation 329/04 to the Personal Health Information Protection Act, 2004, Ontario, and establish the limitations and responsibilities of the service provider with respect to the handling and protection of any personal health information that the service provider may be exposed to during the course of the contracted work.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and AIM Inc. as its Agent.

3.02 This policy applies when third-party services are being contracted with respect to the operations of CytoBase and will require or enable access to CytoBase information.

3.03 The following contracted services are exempt from the requirement for a formal third-party service agreement:

(a) Delivery services of a bonded commercial courier
(b) Paper shredding and disposal services
(c) Computer equipment disposal services
(d) Hardware maintenance and repair

4 RESPONSIBILITY

4.01 It is the responsibility of the President of Inscyte to ensure that Third Party Service Agreements have been executed between Inscyte Corporation and all service providers.

5 DEFINITIONS

5.01 A “third party” is any individual or business entity that is not associated with Inscyte Corporation.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	8 Agreements with Third Party Service Providers		
PS 8.1 Requirement for Third Party Service Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

6 REFERENCES and related POLICIES & PROCEDURES

PS 8.2 Minimum Content of Third Party Service Agreements

PS 8.3 Template Third Party Service Agreements

PS 8.4 Log of Third Party Service Agreements

7 PROCEDURE

7.01 To prepare a new Service Agreement, obtain a template Third Party Service Agreement from AIM's privacy document archives.

7.02 Prior to executing a Service Agreement, provide a copy to the Privacy Officer for review and approval.

7.03 Provide a final copy to the President of Inscyte for signature.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	8 Agreements with Third Party Service Providers		
PS 8.2 Minimum Content of Third Party Service Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 At a minimum, a Third Party Service Agreement shall contain the following information:

(a) Legal names of both parties
(b) Contact information for both parties
(c) Effective date of the agreement
(d) Termination or expiry date of the agreement
(e) A description of the personal health information holdings that the contractee may be expected to handle as part of the service agreement.
(f) The limitations on the collection, use, disclosure and retention of personal health information that the contractee may be expected to handle as part of the service agreement.

1.02 All Third Party Service Agreements shall explicitly identify Inscyte Corporation as a Prescribed Person under regulation 329/04 to the Personal Health Information Protection Act, 2004, Ontario (the Act).

1.03 All Third Party Service Agreements shall include a definition of personal health information as per the Act.

1.04 All Third Party Service Agreements shall attest to the fact that the parties to the agreement have in place privacy and security policies and procedures to safeguard personal health information in compliance with the requirements of the Act and its regulations.

2 PURPOSE

2.01 To inform the service provider about the status of Inscyte Corporation as a Prescribed Person under regulation 329/04 to the Personal Health Information Protection Act, 2004, Ontario, and establish the limitations and responsibilities of the service provider with respect to the handling and protection of any personal health information that the service provider may be exposed to during the course of the contracted work.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and AIM Inc. as its Agent.

3.02 This policy applies when third-party services are being contracted with respect to the operations of CytoBase.

4 RESPONSIBILITY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	8 Agreements with Third Party Service Providers		
PS 8.2 Minimum Content of Third Party Service Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

4.01 It is the responsibility of the Privacy Officer to ensure that Third Party Service Agreements contain the minimum required information.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 8.1 Requirement for Third Party Service Agreements

PS 8.3 Template Third Party Service Agreements

PS 8.4 Log of Third Party Service Agreements

7 PROCEDURE

7.01 To prepare a new Service Agreement, obtain a template Third Party Service Agreement from AIM's privacy document archives.

7.02 Prior to executing a Service Agreement, provide a copy to the Privacy Officer for review and approval.

7.03 Provide a final copy to the President of Inscyte for signature.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	8 Agreements with Third Party Service Providers		
PS 8.3 Template Third Party Service Agreements		Effective:	Nov 1, 2011
		Pages:	
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A standard template Third Party Service Agreement shall be maintained in the privacy documentation archives.

1.02 The template Third Party Service Agreement shall be used to prepare new service agreements.

1.03 The template Third Party Service Agreement shall be updated when:

(a) There is a requirement to change the minimum content of the agreement
(b) There is a change in prevailing legislation or regulations
(c) The Office of the Information and Privacy Commissioner requires a change

1.04 Each template agreement shall be identified with a unique revision number and date of issue.

1.05 Template Third Party Service Agreements shall be approved by the President of Inscyte prior to issue.

2 PURPOSE

2.01 To ensure that Third Party Service Agreements are consistent and include all relevant information so that both Inscyte Corporation and the service provider understand the legal framework and terms and conditions under which service that may expose the contractee to personal health information will be carried out.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and AIM Inc. as its Agent.

3.02 This policy applies when third-party services are being contracted with respect to the operations of CytoBase.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that a current standard template Third Party Service Agreement is maintained in the privacy documentation archives and that this template agreement is used to prepare new service agreements.

4.02 It is the responsibility of the President of Inscyte to review and approve of template Third Party Service Agreements.

5 DEFINITIONS

5.01 None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	8 Agreements with Third Party Service Providers		
PS 8.3 Template Third Party Service Agreements		Effective:	Nov 1, 2011
		Pages:	
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

6 REFERENCES and related POLICIES & PROCEDURES

PS 8.1 Requirement for Third Party Service Agreements

PS 8.2 Minimum Content of Third Party Service Agreements

PS 8.4 Log of Third Party Service Agreements

7 PROCEDURE

7.01 To prepare a new or updated template Third Party Service Agreement, obtain the previous template (if any) from the privacy document archives or start a new template.

7.02 Make modifications to the new template and store it as a "draft" for approval.

7.03 Provide the draft template to the Privacy Officer for review.

7.04 Upon approval of the new template Third Party Service Agreement, increment its revision number, update the issue date, and mark the template as "Final".

7.05 Store the template in the privacy documentation archives, section: Third Party Service Agreements.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	8 Agreements with Third Party Service Providers		
PS 8.4 Log of Third Party Service Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A log of Third Party Service Agreements shall be maintained containing:

(a) The name of the parties to the agreement
(b) The current status of the agreement (active, expired, etc.)
(c) The location where the signed agreement itself is stored
(d) The effective date of the agreement
(e) The termination/expiry date of the agreement
(f) A brief description of the agreement
(g) A brief description of the reason the agreement was terminated (if applicable)

1.02 The log of Third Party Service Agreements shall be updated when:

(a) A new Service Agreement is executed
(b) A Service Agreement expires
(c) A Service Agreement is terminated by either party

2 PURPOSE

2.01 To maintain a perpetual, complete and accurate record of third party service agreements executed between Inscyte Corporation and third parties.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and AIM Inc. as its Agent.

3.02 This policy applies when third-party services are being contracted with respect to the operations of CytoBase.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that the log of Third Party Service Agreements is maintained current, complete and accurate. The Privacy Officer may delegate the updates of the log to designated staff.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 8.1 Requirement for Third Party Service Agreements

PS 8.2 Minimum Content of Third Party Service Agreements

PS 8.3 Template Third Party Service Agreements

7 PROCEDURE

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	8 Agreements with Third Party Service Providers		
PS 8.4 Log of Third Party Service Agreements		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.01 To make a new entry in the log of Third Party Service Agreements or to update an entry, access the log file (Microsoft Excel File) in the privacy document archives, section: Third Party Service Agreements.

7.02 Update the file and save it.

8 REVISION HISTORY

None

9 Data Linkage, De-Identification and Aggregation

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	9 Data Linkage, De-Identification and Aggregation		
PS 9.1 Handling Requests for Data Linkages		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte Corporation may perform linkages of CytoBase with third-party data sources provided that the linkage is permitted under law.

1.02 All requests for linkage of data between CytoBase and a data holding belonging to a third party shall be approved by the President of Inscyte before the linkage can take place.

1.03 Linkage of CytoBase with an external data holding requires a **Data Sharing Agreement** to be executed between Inscyte Corporation and the custodian of the external data holding as per policy PS 7.1 Requirement for Data Sharing Agreements before the data linkage can take place.

1.04 If the information disclosed by Inscyte to the other party as part of the linkage procedure qualifies as personal health information the linkage can only be performed if the other party is a healthcare custodian or a prescribed entity/person under the Personal Health Information Protection Act, 2004, Ontario, and its regulations.

1.05 Data linkages shall be reviewed and approved of by the President of Inscyte prior to the linkage taking place.

2 PURPOSE

2.01 To limit the disclosure and use of information in CytoBase to the purposes for which it was collected and those permitted under Ontario's *Personal Health Information Protection Act, 2004*., and its regulations.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the President of Inscyte Corporation to approve of and execute Data Sharing Agreements with parties requesting data linkages.

4.02 It is the responsibility of the President of Inscyte to review and approve of data linkages before the linkage takes place.

5 DEFINITIONS

5.01 "Data Linkage" refers to the matching of records in CytoBase with records in another data holding, usually using a prescribed set of identifiers (such as health insurance number, surname, date of birth etc.) whereby information from one data holding can be passed on to another. For example, Inscyte may obtain a list of patients from

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	9 Data Linkage, De-Identification and Aggregation		
PS 9.1 Handling Requests for Data Linkages		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

a laboratory and match it to CytoBase to determine the most recent screening date on each patient.

6 REFERENCES and related POLICIES & PROCEDURES

PS 6.1 Limits on Disclosure of PHI

PS 6.2 Disclosure of PHI for Purposes other than Research

PS 6.3 Disclosure of PHI for Research Purposes

PS 7.1 Requirement for Data Sharing Agreements

7 PROCEDURE

7.01 If a request for data linkage is received, refer the request to the President of Inscyte Corporation.

7.02 If the linkage is permitted by law and the President of Inscyte approves of the linkage, prepare a Data Sharing Agreement between Inscyte and the party requesting the linkage.

7.03 If the Data Sharing Agreement is executed, perform the linkage in accordance with the terms and conditions of the Data Sharing Agreement.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	9 Data Linkage, De-Identification and Aggregation		
PS 9.2 De-Identification of PHI – Paper Records		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Printed documents containing personal health information shall be de-identified whenever the personal health information is not required in the document(s) in order to carry out related work.

1.02 Pseudonym values shall be substituted to obfuscate personal health information in printed documents whenever the personal health information is not required in the document(s) in order to carry out related work but placeholders for personal health information are required.

1.03 Agents of Inscyte and employees of AIM shall not use de-identified information, either alone or with other information, to identify and individual.

2 PURPOSE

2.01 To minimize the potential for unauthorized use and/or disclosure of personal health information.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the individual who produces printed documents or receives printed documents to de-identify the documents when personal health information is not required to carry out related work.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures.

6 REFERENCES and related POLICIES & PROCEDURES

PS 9.3 De-Identification of PHI – Digital Records

7 PROCEDURE

7.01 To de-identify a printed document containing personal health information it is acceptable to use an indelible black marker to mask out the elements of personal health information, at minimum:

(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

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	9 Data Linkage, De-Identification and Aggregation		
PS 9.2 De-Identification of PHI – Paper Records		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

(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.

7.02 To produce an obfuscated pseudonym-value document, substitute clearly manufactured/fictitious values for the values of personal health information that are required to be shown in the document. Use the following as guidelines:

Element Name	Pseudonym Value
Patient Name	PatName12
Patent Surname	Surname12
Address	123 Anywhere Street
Telephone Number	555-555-5555
Insurance Number	9999999999
Hospital Name	ABC Hospital
Laboratory Name	ABC Laboratory
Medical Record/Chart Number	MRN1234567

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	9 Data Linkage, De-Identification and Aggregation		
PS 9.3 De-Identification of PHI – Digital Records		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Documents in computer files on fixed disks, portable media or mobile devices containing personal health information shall be de-identified whenever the personal health information is not required in the files in order to carry out related work.

1.02 Pseudonym values shall be substituted for personal health information in computer files whenever the personal health information is not required in order to carry out related work but placeholders for personal health information are required.

1.03 Agents of Inscyte and employees of AIM shall not use de-identified information, either alone or with other information, to identify and individual.

2 PURPOSE

2.01 To minimize the potential for unauthorized use and/or disclosure of personal health information.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the individual who produces digital documents or receives digital documents to de-identify the documents when personal health information is not required to carry out related work.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures.

6 REFERENCES and related POLICIES & PROCEDURES

PS 9.2 De-Identification of PHI – Paper Records

7 PROCEDURE

7.01 To de-identify a digital document containing personal health information it is acceptable to replace the values of personal health information with NULL values or a string of "X" character matching the length of the original data. For example, a patient surname may be replaced with "XXXXXXXX" which will maintain its position in the document, or a NULL value which will eliminate the information altogether. This technique should be applied to all elements of personal health information such as:

(a) Patient name, middle name and last name

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	9 Data Linkage, De-Identification and Aggregation		
PS 9.3 De-Identification of PHI – Digital Records		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

(b) Patient contact information (address, city, postal code, telephone etc.)
(c) Patient health insurance numbers
(d) Patient medical record numbers and/or chart numbers
(e) Specimen accession numbers and/or medical report identifiers
(f) Originating institution/hospital name

7.02 To produce a pseudonym-value digital document, substitute generic values for the values of personal health information that are required to be shown in the document. Use the following guidelines:

Element Name	Pseudonym Value
Patient Name	PatName12
Patent Surname	Surname12
Address	123 Anywhere Street
Telephone Number	555-555-5555
Insurance Number	9999999999
Hospital Name	ABC Hospital
Laboratory Name	ABC Laboratory
Medical Record/Chart Number	MRN1234567

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	9 Data Linkage, De-Identification and Aggregation		
PS 9.4 Limits on Aggregation of Data (Statistics)		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 It is acceptable to produce and disclose aggregated information from the information in CytoBase provided that the aggregated information does not identify, or cannot be used to identify an individual.

1.02 Aggregate information with fewer than five (5) observations per aggregation is not to be disclosed. Prior to the disclosure of any aggregated information, the Privacy Officer shall review the information to assess the risk of 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 the purpose of the disclosure. If the risk is deemed inappropriate the information shall not be disclosed. In assessing the risk of inadvertent disclosure, the Privacy Officer shall have regard to section 4(2) of Ontario's *Personal Health Information Protection Act, 2004*, 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.

1.03 Agents of Inscyte or employees of AIM shall not use aggregate information, either alone or with other information, to identify an individual.

2 PURPOSE

2.01 To minimize the potential for unauthorized use and/or disclosure of personal health information.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of each individual preparing aggregated data to be vigilant of the potential for the information to be used to identify an individual.

4.02 It is the responsibility of the Privacy Officer to review aggregated data and assess the risk of inadvertent disclosure of identity resulting from a small number of observation or the localization of the observations before the data are disclosed.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures.

6 REFERENCES and related POLICIES & PROCEDURES

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	9 Data Linkage, De-Identification and Aggregation		
PS 9.4 Limits on Aggregation of Data (Statistics)		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 6.1 Limits on Disclosure of PHI

PS 6.2 Disclosure of PHI for Purposes other than Research

PS 6.3 Disclosure of PHI for Research Purposes

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

10 Privacy Audit Program

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	10 Privacy Audit Program		
PS 10.1 Conducting Privacy Impact Assessments		Effective:	Nov 1, 2011
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte Corporation shall conduct a **Privacy Impact Assessment** in respect to the operations of the CytoBase system 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.

1.02 Privacy Impact Assessments may not be required when making **routine upgrades, repairs , or changes** to the CytoBase information and security infrastructure provided that these changes do not materially alter or degrade the privacy and/or security measures in place at the time. Such circumstances may include:

(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.)

Under these circumstances a risk assessment shall be conducted to determine if the changes will have a negative impact before the changes are put into place and a determination will be made whether or not the changes warrant a Privacy Impact Assessment.

1.03 When required, Privacy Impact Assessments shall be conducted, and any recommended remedial or corrective actions shall be taken, and the Privacy Impact Assessment shall be amended, before any proposed changes giving rise to the Privacy Impact Assessment are implemented.

1.04 The results of the most recent Privacy Impact Assessment shall be published on Inscyte Corporation's website and made openly available to the public.

1.05 All Privacy Impact Assessment documentation shall be retained in a **Log of Privacy Impact Assessments** in perpetuity in the privacy documentation archives.

1.06 At minimum, a **Privacy Impact Assessment** must describe:

(a) The data holding, information system, technology or program at issue;

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	10 Privacy Audit Program		
PS 10.1 Conducting Privacy Impact Assessments		Effective:	Nov 1, 2011
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

(b) The nature and type of personal health information collected, used or disclosed or that is proposed to be collected, used or disclosed;
(c) The sources of the personal health information;
(d) The purposes for which the personal health information is collected, used or disclosed or is proposed to be collected, used or disclosed;
(e) The reason that the personal health information is required for the purposes identified;
(f) The flows of the personal health information;
(g) The statutory authority for each collection, use and disclosure of personal health information identified;
(h) The limitations imposed on the collection, use and disclosure of the personal health information;
(i) Whether or not the personal health information is or will be linked to other information;
(j) The retention period for the records of personal health information;
(k) The secure manner in which the records of personal health information are or will be retained, transferred and disposed of;
(l) 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;
(m) 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;
(n) Recommendations to address and eliminate or reduce the privacy risks identified; and
(o) The administrative, technical and physical safeguards implemented or proposed to be implemented to protect the personal health information.

2 PURPOSE

2.01 To obtain a professional assessment of the impact on privacy that may result from a significant change in the operational environment of CytoBase or the scope of use of CytoBase information.

2.02 To communicate to the public how the privacy of personal health information is protected and secured against unauthorized access and disclosure.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and AIM Inc. as its Agent.

4 RESPONSIBILITY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	10 Privacy Audit Program		
PS 10.1 Conducting Privacy Impact Assessments		Effective:	Nov 1, 2011
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

4.01 It is the responsibility of the President on Inscyte Corporation to undertake a Privacy Impact Assessment when a significant change in the operational environment of CytoBase, or the scope of use of CytoBase information occurs. The President may delegate this work to designated staff or third party service provider.

4.02 It is the responsibility of the Privacy Officer to ensure that the most recent Privacy Impact Assessment is published on Inscyte Corporation's website and made available to the public.

4.03 It is the responsibility of the Privacy Officer to ensure that all Privacy Impact Assessments are retained in the privacy document archives.

4.04 It is the responsibility of the Security Officer to prepare risk assessments when changes to the CytoBase computing and security infrastructure are contemplated and to report the findings to the Privacy Officer. It is the responsibility of the Security Officer to document the findings in the Asset Inventory.

4.05 It is the responsibility of the Privacy Officer to review risk assessment findings when changes to the CytoBase computing and security infrastructure are contemplated and determine whether or not a Privacy Impact Assessment is warranted. It is the responsibility of the Privacy Officer to document the reasons for the determination in the Asset Inventory.

5 DEFINITIONS

5.01 A Privacy Impact Assessment ("PIA") is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal health information. It also defines the measures used to mitigate and, wherever possible, eliminate the identified risks. The PIA process ensures that measures intended to protect privacy and ensure the confidentiality and security of personal health information are considered at the outset of any new program or service delivery initiative. A PIA also communicates to the public how their privacy is protected and their information kept confidential and secure from unauthorized access.

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.1 Publication of these Policies and Procedures

PS 10.1 Conducting Privacy Impact Assessments

PS 17.2 Asset Inventory and Configuration Information

7 PROCEDURE

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	10 Privacy Audit Program		
PS 10.1 Conducting Privacy Impact Assessments		Effective:	Nov 1, 2011
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	10 Privacy Audit Program		
PS 10.2 Log of Privacy Impact Assessments		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A **Log of Privacy Impact Assessments** shall be maintained in perpetuity in the privacy document archives to record, track and describe the outcomes of each assessment. The minimum information content for each audit log entry shall be:

(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/outcome of the recommendations

1.02 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.

2 PURPOSE

2.01 To monitor the privacy program and document archives for completeness and accuracy and ensure that day to day operations are in compliance with these Privacy & Security Policies and Procedures.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	10 Privacy Audit Program		
PS 10.2 Log of Privacy Impact Assessments		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to initiate a Privacy Audit.

5 DEFINITIONS

5.01 A "Privacy Audit" is a self-assessment tool. The purpose of the audit is to review and collect information that can inform the planning and decision-making process regarding the on-going application of privacy legislation to the organization.

6 REFERENCES and related POLICIES & PROCEDURES

PS 1.2 Review of Policies and Procedures

PS 10.1 Conducting Privacy Impact Assessments

PS 10.5 Auditing Computer Servers

PS 10.6 Auditing Employee Computers and Workspaces

PS 10.4 Log of Privacy Audits

PS 15.1 Conducting Security Audits

7 PROCEDURE

7.01 When undertaking an annual Privacy Audit, review the status of required documentation and privacy logs in the privacy document archives.

7.02 After the Privacy Audit is completed, make an new entry in the Log of Privacy audits to record the activity and its outcomes.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	10 Privacy Audit Program		
PS 10.3 Conducting Privacy Audits		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte Corporation shall conduct internal privacy audits every year to ascertain the current state of its personal health information holdings and related policies and procedures. This activity may be carried out in parallel with the annual review of the Privacy & Security Policies and Procedures.

1.02 The annual privacy audit will involve:

(a) Reviewing changes to applicable legislation and applicable orders 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

2 PURPOSE

2.01 To monitor the privacy program and document archives for completeness and accuracy and ensure that day to day operations are in compliance with these Privacy & Security Policies and Procedures.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	10 Privacy Audit Program		
PS 10.3 Conducting Privacy Audits		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to initiate a Privacy Audit.

5 DEFINITIONS

5.01 A "Privacy Audit" is a self-assessment tool. The purpose of the audit is to review and collect information that can inform the planning and decision-making process regarding the on-going application of privacy legislation to the organization.

6 REFERENCES and related POLICIES & PROCEDURES

PS 1.2 Review of Policies and Procedures

PS 3.2 Privacy Document Archives

PS 10.5 Auditing Computer Servers

PS 10.6 Auditing Employee Computers and Workspaces

PS 10.4 Log of Privacy Audits

PS 15.1 Conducting Security Audits

7 PROCEDURE

7.01 When undertaking an annual Privacy Audit, review the status of required documentation and privacy logs in the privacy document archives.

7.02 After the Privacy Audit is completed, make an new entry in the Log of Privacy Audits to record the activity and its outcomes.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	10 Privacy Audit Program		
PS 10.4 Log of Privacy Audits		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A Log of Privacy Audits shall be maintained in perpetuity to record and describe the outcomes of each audit activity. The minimum information content for each audit log entry shall be:

2 PURPOSE

2.01 To keep a perpetual record of activities performed to audit the privacy program and detect possible breaches of privacy.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that an accurate and complete Log of Privacy Audits is maintained.

4.02 It is the responsibility of the person carrying out an audit activity to ensure that the activity is recorded in the Log of Privacy Audits.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.2 Privacy Document Archives

PS 10.3 Conducting Privacy Audits

PS 10.5 Auditing Computer Servers

PS 10.6 Auditing Employee Computers and Workspaces

PS 11.2 Reporting a Breach of Privacy

7 PROCEDURE

7.01 The Log of Privacy Audits can be found in AIM's privacy document archives, section: Log of Privacy Audits, on AIM's business network.

7.02 To make an entry in the log, open the Microsoft Excel file named Log of Privacy Audits and add an entry to the list.

7.03 Notify the Privacy Officer when an update to the log is made.

8 REVISION HISTORY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	10 Privacy Audit Program		
PS 10.4 Log of Privacy Audits		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	
None			

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	10 Privacy Audit Program		
PS 10.5 Auditing Computer Servers		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A monthly audit shall be performed of computer server and storage networks to ascertain if any files containing personal health information are located outside of secured computing environments.

1.02 Computer servers or storage networks that are dedicated to the secure storage of personal health information need not be audited.

2 PURPOSE

2.01 To detect and contain breaches of privacy.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that monthly audits of computer servers are preformed and each audit inspection is recorded in the Log of Privacy Audits.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures.

6 REFERENCES and related POLICIES & PROCEDURES

PS 10.3 Conducting Privacy Audits

PS 10.6 Auditing Employee Computers and Workspaces

PS 10.4 Log of Privacy Audits

7 PROCEDURE

7.01 Once per month, select a computer server that is not dedicated to the storage of personal health information at random.

7.02 Perform a search of the server and storage network to identify files that match the following criteria:

(a) Filenames with an extension of: HL7, XML, and TXT
(b) Files containing any of the following strings (in either upper or lower case):

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	10 Privacy Audit Program		
PS 10.5 Auditing Computer Servers		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

ACCESSION, CY, GY, SP, DOB, DATE OF BIRTH, FIRST NAME, LAST NAME, SURNAME, HIN, PHIN, MRN, MSH, OBR, OBX, PID, SEX, SPECIMEN, RPT, PATHOLOGY, CYTOLOGY, HOSPITAL, REPORT ID, PATIENT ID.

7.03 Perform a search for files with the extension MDB, DBF or DAT to identify any local database files.

7.04 Examine all of the files that were found in the previous steps to ascertain if these contain personal health information.

7.05 Log the activity in the Log of Privacy Audits in the privacy document archives.

7.06 If files of personal health information are detected in a unsecured environment, prepare a Privacy Breach Report as per policy PS 11.2 Reporting a Breach of Privacy

7.07 Either transfer the files to a secure location or dispose of the files containing personal health information in accordance with the disposal policies.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	10 Privacy Audit Program		
PS 10.6 Auditing Employee Computers and Workspaces		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A monthly audit shall be performed of a randomly selected employee workstation and/or laptop to ascertain if any files containing personal health information are located outside of secured computing environments.

1.02 A monthly inspection of a randomly selected employee workspace shall be conducted to determine if any personal health information in printed form or on portable media is located outside of secured premises.

2 PURPOSE

2.01 To detect and contain breaches of privacy.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that monthly audits of workstations and laptops are preformed and that each audit inspection is recorded in the Log of Privacy Audits.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures.

6 REFERENCES and related POLICIES & PROCEDURES

PS 10.3 Conducting Privacy Audits

PS 10.5 Auditing Computer Servers

PS 10.4 Log of Privacy Audits

7 PROCEDURE

7.01 Once per month, select an employee and/or workstation at random.

7.02 Perform a search of employee's workstation or laptop to find files that match the following criteria:

(a) Filenames with an extension of: HL7, XML, and TXT
(b) Files containing any of the following strings (in either upper or lower case):

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	10 Privacy Audit Program		
PS 10.6 Auditing Employee Computers and Workspaces		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

ACCESSION, CY, GY, SP, DOB, DATE OF BIRTH, FIRST NAME, LAST NAME, SURNAME, HIN, PHIN, MRN, MSH, OBR, OBX, PID, SEX, SPECIMEN, RPT, PATHOLOGY, CYTOLOGY, HOSPITAL, REPORT ID, PATIENT ID.

7.03 Perform a search for files with the extension MDB, DBF or DAT to identify any local database files.

7.04 Examine all of the files that were found in the previous steps to ascertain if these contain personal health information.

7.05 Inspect the employee's workspace and determine if there are any documents in printed format or on portable media or mobile devices that might contain personal health information.

7.06 Log the activity in the Log of Privacy Audits in the privacy document archives.

7.07 If personal health information is found in a unsecured environment, prepare a Privacy Breach Report as per policy PS 11.2 Reporting a Breach of Privacy

7.08 Either transfer the files/media to a secure location or dispose of the files containing personal health information in accordance with policies governing the disposal and destruction of personal health information.

8 REVISION HISTORY

None

11 Handling of Privacy Breaches, Complaints and Inquiries

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.1 Indentifying a Breach of Privacy		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A privacy breach occurs whenever a person has contravened or is about to contravene a provision of Ontario's *Personal Health Information Protection Act, 2004* (the Act) or its regulations, including section 12(1) of the Act.

1.02 A breach of privacy may be reported via a privacy complaint or challenge to compliance with these policies and procedures filed by a third party.

1.03 A breach of privacy may be self-identified through the course of everyday work.

1.04 Subject to the definition below, a breach of privacy or a potential breach may be signaled by the discovery that:

(a) Personal health information is found in an unexpected context, location, quantity, or format.
(b) Privacy & Security Policies and Procedures are not being (or have not been) adhered to.
(c) Contractual terms and conditions regarding the handling of personal health information are not being (or have not been) adhered to.

1.05 Any individual who identifies a breach of privacy shall report the incident to the Privacy Officer and the Security officer as soon as possible and in accordance with policy and procedure: PS 11.2 Reporting a Breach of Privacy.

1.06 The first course of action upon discovering a breach of privacy is to contain the breach in accordance with policy and procedure: PS 11.3 Actions Following a Breach of Privacy

2 PURPOSE

2.01 To provide a definition of a breach of privacy and describe the circumstances that may signal that a breach of privacy has occurred or may occur.

2.02 To foster an environment where every individual is vigilant and proactive with respect to safeguarding personal health information.

2.03 Section 12(1) of the Act requires Inscyte Corporation, and by extension AIM Inc. as agent of Inscyte, to take steps that are reasonable in the circumstances to ensure personal health information is protected against theft, loss and unauthorized use or disclosure, and to ensure that records containing personal health information are protected against unauthorized access, copying, modification or disposal.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.1 Indentifying a Breach of Privacy		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

4 RESPONSIBILITY

4.01 It is the responsibility of each member of the staff of Inscyte Corporation and its agents to be vigilant of and identify breaches (or potential breaches) of privacy and report these as soon as possible so that a breach of privacy can be contained and managed, and that mitigating actions can be taken to prevent similar breaches from occurring in the future.

5 DEFINITIONS

5.01 A **Breach of Privacy** is defined 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 these *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 staff and *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.

5.02 A breach of privacy occurs in the above circumstances regardless of the severity of the consequences of the breach.

6 REFERENCES and related POLICIES & PROCEDURES

PS 11.2 Reporting a Breach of Privacy

PS 11.3 Actions Following a Breach of Privacy

PS 11.4 Log of Privacy Breaches

PS 11.5 Handling Privacy Complaints

PS 16.1 Identifying a Breach

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.2 Reporting a Breach of Privacy		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Any individual who discovers a breach or potential breach of privacy shall contact the Privacy Officer and the Security Officer verbally or in writing to report the incident as soon as possible.

1.02 A Privacy Breach Report shall be initiated for each incident of breach within five (5) business days of notification.

1.03 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, further notification will be given to:

(a) The President of Inscyte
(b) Affected healthcare custodians (member laboratories) so that the persons to whom the personal health information applies can be notified about the breach, pursuant to the provisions of subsection 12(2) of Ontario's *Personal Health Information Protection Act, 2004*.
(c) The Office of the Information and Privacy Commissioner of Ontario.

2 PURPOSE

2.01 To ensure breaches of privacy are reported to the appropriate parties and in accordance with legislative requirements, including, but not limited to Ontario's *Personal Health Information Protection Act, 2004* (the Act).

2.02 To document breaches of privacy with sufficient information so that mitigating actions can be taken to prevent similar breaches from occurring in the future.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of each member of the staff of Inscyte Corporation and its agents to identify breaches (or potential breaches) of privacy and report these as soon as possible so that actions can be taken to contain the breach and mitigating actions taken to prevent similar breaches from occurring in the future.

4.02 It is the responsibility of the Privacy Officer to notify the President of reported breaches and ensure that all breaches are fully documented.

4.03 It is the responsibility of the President of Inscyte Corporation to notify the Board of Directors, member laboratories, and the Office of the Information and Privacy Commissioner, Ontario about breaches as appropriate.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.2 Reporting a Breach of Privacy		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

5 DEFINITIONS

5.01 See definition of a breach of privacy in policy: PS 11.1 Indentifying a Breach of Privacy

6 REFERENCES and related POLICIES & PROCEDURES

PS 11.1 Indentifying a Breach of Privacy

PS 11.3 Actions Following a Breach of Privacy

PS 11.4 Log of Privacy Breaches

PS 16.2 Reporting a Breach of Security

7 PROCEDURE

7.01 To prepare a **Privacy Breach Report**, access AIM's PS 3.2 Privacy Document Archives, Section: Log of Privacy Breaches and open a Breach Report template. Fill out the report as completely as possible. Send the report to the Privacy Officer for review and approval.

7.02 In all cases of breach initiate policy and procedure PS 11.3 Actions Following a Breach of Privacy

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.3 Actions Following a Breach of Privacy		Effective:	Nov 1, 2011
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 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
8. Approve report and recommendations for mitigating strategies

Depending on the severity of the breach, these actions may have to be undertaken simultaneously, or in very short succession. Refer to the procedures below for details on these steps.

2 PURPOSE

2.01 To respond quickly, effectively and in a coordinated manner in case of a breach of privacy.

2.02 To contain the breach and thereby limit the severity of the consequences.

2.03 To document the breach and make remediation efforts easier.

2.04 To prepare for the potential involvement of the Office of the Information and Privacy Commissioner, Ontario.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of each and every employee to implement the actions following a breach of privacy (i.e. the breach protocol) immediately upon discovering a breach of privacy or suspected breach of privacy.

5 DEFINITIONS

5.01 See definition of a **Breach of Privacy** in policy: PS 11.1 Indentifying a Breach of Privacy

6 REFERENCES and related POLICIES & PROCEDURES

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.3 Actions Following a Breach of Privacy		Effective:	Nov 1, 2011
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 11.1 Indentifying a Breach of Privacy

PS 11.2 Reporting a Breach of Privacy

PS 11.4 Log of Privacy Breaches

PS 16.3 Actions Following a Breach of Security

7 PROCEDURE

7.01 **Notify Appropriate Personnel** – In all incidents of breach or suspected breach, notify the Privacy Officer. Also:

(a) Notify AIM's President and CEO if the breach appears to have been perpetrated by theft, loss, or unauthorized access to AIM's computer systems.
(b) Notify AIM's technical services department if the breach appears to have been perpetrated by unauthorized access to AIM's premises or computer systems.
(c) Notify AIM's technical services department and affected customers if the breach is indicative of a process failure in the collection/transfer/retention/disclosure of personal health information.
(d) Notify AIM's technical services department if the breach is indicative of a process failure in the disposal/destruction of personal health information.

7.02 **Assess the Incident** – Assess the incident of breach and determine the type of personal health information involved, the volume of the information, its format, and its location. Determine the likely cause of the breach (accidental, intentional) and the mechanism of the breach. Assess the likelihood that the personal health information has been disclosed to unauthorized parties, or the likelihood that it may be disclosed in future.

If there is reasonable cause to believe that personal health information has or is likely to be disclosed to unauthorized parties, notify the President of Inscyte and notify affected custodians/providers of the information in question that a breach of privacy has occurred.

7.03 **Contain the Breach** – Attempt to recover and secure (or destroy) the personal health information that has been disclosed or may be disclosed. This might include gathering and shredding paper records, recovering portable media or mobile computing devices., erasing files from computer disks, destroying tapes or CDs, and so on.

7.04 **Notify Affected Parties** – Following containment actions, if there is reasonable cause to believe that personal health information has or is likely to be disclosed to unauthorized parties, subsection 12(2) of Ontario's *Personal Health Information Protection Act, 2004* requires that efforts be made to contact the affected people

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.3 Actions Following a Breach of Privacy		Effective:	Nov 1, 2011
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

and inform them of the breach. Notify the Office of the Information and Privacy Commissioner of Ontario (IPC) of the breach and seek direction on further actions. Inform each affected member laboratory about the breach so that the laboratory may communicate with the patient.

7.05 **Prepare a Report of the Breach** – Acquire the template Breach Report from AIM's PS 3.2 Privacy Document Archives, Section: Log of Privacy Breaches, and prepare a report of the breach. Forward the report to the Privacy Officer and Security Officer for review.

7.06 **Investigate and Remediate** – Investigate the circumstances and motivation behind the breach. The Breach Report should contain information on the cause and/or reason for the breach, and recommendations for remediation measures to mitigate or prevent similar breaches from occurring in the future.

7.07 **Finalize and Archive the Breach Report** – Send the final Breach Report to the Privacy Officer for sign-off. Upon sign-off the Privacy Officer will distribute the report to all stakeholders involved and retain a read-only copy (PDF) in AIM's privacy and security document archives.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.4 Log of Privacy Breaches		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A perpetual Log of Privacy Breaches shall be maintained that describes each incident of breach in the form of a **Privacy Breach Report**.

1.02 A **Privacy Breach Report** shall contain the following minimum information:

(a) The date the breach was reported to Inscyte
(b) The name of the person(s) reporting the breach
(c) The name of the author(s) of the report (investigators)
(d) The date/time of the breach incident (or estimate thereof)
(e) The evidence of an incident of breach (what lead to the discovery of breach)
(f) The nature/source of the personal health information involved
(g) The amount of personal health information involved (or estimate thereof)
(h) The format of the personal health information (paper, media, etc.)
(i) The location of the personal health information
(j) 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
(k) Who perpetrated the breach
(l) The motivation/cause for the breach
(m) The mechanism of the breach (i.e. method, process failure, etc.)
(n) Containment procedure (what was done to contain the breach)
(o) Likelihood of disclosure of personal health information to unauthorized parties
(p) List of parties and personnel contacted/notified
(q) Indication if affected persons were contacted (names & dates)
(r) Indication if IPC was contacted (date)
(s) Remedial actions taken and recommendations for mitigating strategies
(t) Sign-off/approval name, title and date

1.03 To finalize a **Privacy Breach Report**, the report shall be reviewed and signed-off by the Privacy Officer.

2 PURPOSE

2.01 To document each incident of a breach of privacy for future reference.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.4 Log of Privacy Breaches		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

2.02 To provide a record of remedial actions and mitigation strategies to prevent similar occurrences in the future.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that the Log of Privacy Breaches is complete and up-to-date.

5 DEFINITIONS

5.01 See definition of a breach of privacy in: PS 11.1 Indentifying a Breach of Privacy

6 REFERENCES and related POLICIES & PROCEDURES

PS 11.1 Indentifying a Breach of Privacy

PS 11.2 Reporting a Breach of Privacy

PS 11.3 Actions Following a Breach of Privacy

PS 16.4 Log of Security Breaches

7 PROCEDURE

7.01 To prepare a **Privacy Breach Report** acquire the template breach report from AIM's privacy and security document archives and fill out the report. Send the report to the Privacy Officer for review and approval.

7.02 Use the following **file naming** convention to distinguish each breach report:

PBR-<*incident date*>-<*incident name*>.doc

Where:

PBR-	The standard prefix for Privacy Breach Report
<*incident date*>	The date of discovery in the form yyyy-mm-dd
<*incident name*>	A short name for the incident
Example:	PBR-2011-05-14- Misplaced CytoBase Tape.doc

7.03 When a breach report is completed, convert the document to a **read-only file** format (such as Adobe PDF) with the same file name.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.5 Handling Privacy Complaints		Effective:	Nov 1, 2011
		Pages:	4
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 An individual shall be able to address a challenge concerning compliance with Inscyte Corporation's Privacy & Security Policies and Protocols to the President and/or the Privacy Officer of Inscyte Corporation.

1.02 Inscyte Corporation will investigate all complaints and will inform individuals who make inquiries or lodge complaints of the relevant complaint resolution process.

1.03 If a complaint is deemed justified, Inscyte Corporation will take appropriate measures to remediate and resolve the complaint including, if necessary, amending its Privacy & Security Policies and Procedures.

1.04 In addition, an individual will be able to address a challenge concerning compliance by Inscyte Corporation with these policies and procedures by making a complaint to the Office of the Information and Privacy Commissioner of Ontario at:

Information and Privacy Commissioner/Ontario
2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Telephone: 416-326-3333 or 1-800-387-0073

1.05 Inscyte Corporation's standard complaint form shall be used and made freely available to the public via download from Inscyte Corporation's website.

1.06 The President of Inscyte Corporation shall be notified about each complaint received and about the complaint and will notify any related parties to the complaint, which may include ministries of government and the Office of the Information and Privacy Commissioner of Ontario.

1.07 Complaints regarding access to personal health information or the accuracy thereof shall not be referred to the Office of the Information and Privacy Commissioner of Ontario.

1.08 All complaints shall be investigated in a timely manner, which may involve seeking additional information from the complainant and consultation with affected parties. A written report shall be prepared describing the results of the investigation with recommendations for actions 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.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.5 Handling Privacy Complaints		Effective:	Nov 1, 2011
		Pages:	4
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1.09 All complaints shall be documented and retained in perpetuity in AIM's privacy and security document archives (see: PS 11.6 Log of Privacy Complaints for details on the minimum content and retention of standard Privacy Compliance Challenge Forms and Complaint Investigation and Resolution Forms).

2 PURPOSE

2.01 To provide an open and unobstructed mechanism for the general public to lodge a complaint against Inscyte Corporation (or its Agents) regarding compliance with its Privacy & Security Policies and Procedures.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that complaints received are documented and communicated to all affected parties, including the Healthcare custodians from whom the personal health information originated.

4.02 It is the responsibility of the President of Inscyte to approve recommended actions to be taken to resolve a complaint.

4.03 It is the responsibility of the Privacy Officer to inform the complainant about actions taken to resolve the complaint.

5 DEFINITIONS

5.01 A **Privacy Complaint** is 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.

6 REFERENCES and related POLICIES & PROCEDURES

PS 11.6 Log of Privacy Complaints

7 PROCEDURE

7.01 If an individual asks for instructions about lodging a complaint, provide the individual with a paper (or electronic) copy of the **Privacy Compliance Challenge Form** and instructions for filling out and lodging the complaint. These forms and instructions can be found in the PS 3.2 Privacy Document Archives, Section: Log of Privacy Complaints.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.5 Handling Privacy Complaints		Effective:	Nov 1, 2011
		Pages:	4
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.02 Upon receipt of a **Privacy Compliance Challenge Form** from an individual, inform the Privacy Officer about the new complaint. Store an electronic copy of the complaint in AIM's PS 3.2 Privacy Document Archives, Section: Log of Privacy Complaints.

7.03 Forward a copy of the complaint to the President of Inscyte Corporation. Also forward a copy to the Office of the Information and Privacy Commissioner of Ontario provided the complaint is not a question of access to or accuracy of CytoBase information.

7.04 If the complaint is in regards to the operations of a specific member laboratory in CytoBase system forward a copy of the complaint to the cytology laboratory manager at the member laboratory.

7.05 Open a new **Complaint Investigation and Resolution Form** by using the template found in AIM's privacy document archives, Section: Log of Privacy Complaints. Copy the complaint information into the form.

7.06 Perform an investigation of the complaint. The purpose of the investigation is to determine the circumstances surrounding the complaint and to validate the complaint. Document the actions performed during the investigation, who performed these actions and when and note the dates and time of any contact with third parties or the complainant made during the investigation. Also document the results and/or outcomes of the investigation.

7.07 Devise and document recommended actions to resolve the complaint, noting specifically any changes to procedures/policies or the technical properties of the affected systems that may be required to prevent similar occurrences in the future.

7.08 Forward a copy of the Complaint Investigation and Resolution Form to the Privacy Officer for a review of the investigation, its outcomes, and approval of the recommended resolution. Forward a copy to the President of Inscyte. Provided that the complaint is not a question of access to or accuracy of CytoBase information, also send a copy to the Office of the Information and Privacy Commissioner of Ontario.

7.09 If the recommended actions for resolving the complaint are approved, forward a copy of the Complaint Investigation and Resolution Form to the complainant and contact the complainant to discuss the actions that will be taken to resolve the complaint.

7.10 Carry out the recommended actions for resolving the complaint and finalize the Complaint Investigation and Resolution Form.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.5 Handling Privacy Complaints		Effective:	Nov 1, 2011
		Pages:	4
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.11 Obtain sign-off from the Privacy Officer and send a copy to the President of Inscyte. Provided that the complaint is not a question of access to or accuracy of CytoBase information, also send a copy to the Office of the Information and Privacy Commissioner of Ontario.

7.12 Ensure that a read-only (PDF) copy of the Complaint Investigation and Resolution Form is retained in AIM's PS 3.2 Privacy Document Archives, Section: Log of Privacy Complaints.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.6 Log of Privacy Complaints		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A perpetual Log of Privacy Complaints shall be maintained documenting complaints received, investigations undertaken, results, recommended actions and resolutions.

1.02 A standard **Privacy Compliance Challenge Form** shall be prepared and made available to allow individuals to easily file complaints. This form shall contain the following minimum information:

(a) The date of the complaint
(b) The name of the complainant
(c) The contact/address information of the complainant
(d) A detailed description of the complaint

1.03 The Log of Privacy Complaints shall include a copy of all Privacy Compliance Challenge Forms received, each with a matching **Complaint Investigation and Resolution Form** containing the following minimum information:

(a) The date of the complaint
(b) The name of the complainant
(c) The contact/address information of the complainant
(d) A detailed description of the complaint
(e) The date of the investigation (start date)
(f) The name/title of the principle investigator
(g) A description of the investigation performed and results/outcomes
(h) A description of recommended actions for resolving the complaint
(i) Description of the final resolution
(j) The resolution date
(k) Sign-off date
(l) Name/title of authorized signing individual (i.e. Privacy Officer)

2 PURPOSE

2.01 To maintain a complete record of privacy complaints received and the actions taken to investigate and resolve each complaint.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that the Log of Privacy Complaints is complete and up-to-date.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.6 Log of Privacy Complaints		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 11.5 Handling Privacy Complaints

PS 3.2 Privacy Document Archives

7 PROCEDURE

7.01 To prepare a **Privacy Challenge Complaint Form** acquire the template from the privacy document archives and fill out the form.

7.02 To prepare a **Complaint Investigation and Resolution Form** acquire the template from AIM's privacy document archives and fill out the form.

7.03 Use the following **file naming** convention to distinguish each complaint:

<prefix>-<*complainant*>-<*complaint date*>.doc

Where:

<prefix>	"PC" for the Privacy Challenge Complaint Form
	"PCR" for the Complaint Investigation and Resolution Form
<*complainant*>	The name of the person filing the complaint
<*complaint date*>	The date of the complaint in the form yyyy-mm-dd
Example:	PC- 2011-05-14-Nora Jones.doc
	PCR-2011-05-14- Nora Jones.doc

7.04 When a complaint is resolved, convert the document to a **read-only file** format (such as Adobe PDF) with the same file name.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.7 Handling Privacy Inquiries		Effective:	Nov 1, 2011
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 An individual shall be able to address an inquiry regarding Inscyte Corporation's Privacy & Security Policies and Procedures and related to Inscyte's compliance with the Act and its regulation to the Privacy Officer of Inscyte Corporation.

1.02 Inscyte Corporation will respond to all inquiries and will inform individuals who make inquiries of the inquiry process.

1.03 Inscyte Corporation's standard **Privacy Inquiry Form** shall be used and made freely available to the public via download from Inscyte Corporation's website.

1.04 All inquiries shall be responded to in a timely manner, which may involve seeking additional information from the inquirer and consultation with affected parties. A written **Response Letter** shall be prepared to each inquiry. The response shall be provided to the inquirer, the President of Inscyte and all related parties.

1.05 All inquires and responses shall be documented and retained in perpetuity in a **Log of Privacy Inquiries** located in the privacy and security document archives, containing 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

2 PURPOSE

2.01 To provide an open and unobstructed mechanism for the general public to inquire about Inscyte's privacy practices and its compliance with the Act and its regulation.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that inquiries received are logged, documented and responded to in a timely manner.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.7 Handling Privacy Inquiries		Effective:	Nov 1, 2011
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

4.02 It is the responsibility of the Privacy Officer to delegate activities to appropriate individuals to prepare a response and to review and approve the response before a response Letter is delivered to the inquirer.

5 DEFINITIONS

5.01 A **Privacy Inquiry** is 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.

6 REFERENCES and related POLICIES & PROCEDURES

PS 11.5 Handling Privacy Complaints

7 PROCEDURE

7.01 If an individual asks for instructions about making an inquiry, provide the individual with a paper (or electronic) copy of the **Privacy Inquiry Form** and instructions for filling out the form. These forms and instructions can be found in the PS 3.2 Privacy Document Archives, Section: Log of Privacy Inquiries.

7.02 Upon receipt of a **Privacy Inquiry Form** from an individual, inform the Privacy Officer about the inquiry. Make an entry a new entry in the Log of Privacy Inquiries assigning a new inquiry identification number and store an electronic copy of the Privacy Inquiry Form in the PS 3.2 Privacy Document Archives, Section: Log of Privacy Inquiries.

7.03 It is the responsibility of the Privacy Officer to delegate activities to be carried out in preparing a response to the inquiry, which may include document reviews, seeking additional information from the inquirer, and consultation with affected parties, and to set out the time frame in which the response is to be prepared.

7.04 Inform the inquirer that a response is being prepared and the anticipated date on which it will be completed.

7.05 Prepare a Letter of Response citing the Inquiry identification number, date and the name of the inquirer, and a summary of the inquiry. Describe the response to the inquiry in the letter.

7.06 Provide a copy of the Response Letter to the Privacy Officer for review and approval.

7.07 If the Response Letter is approved, deliver a copy to the inquirer and update the Log of Privacy Inquiries with the date of response, the name of the respondent and a summary of the response.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	11 Handling of Privacy Breaches, Complaints and Inquiries		
PS 11.7 Handling Privacy Inquiries		Effective:	Nov 1, 2011
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.08 Ensure that a read-only (PDF) copy of the Response Letter is retained in AIM's PS 3.2 Privacy Document Archives, Section: Log of Privacy Inquiries.

8 REVISION HISTORY

None

12 Physical Security

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.1 Physical Isolation of Personal Health Information		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal health information in any format or storage medium shall be stored and used in secured premises that require passing through at least two physical security checkpoints.

2 PURPOSE

2.01 To prevent unauthorized access to personal health information.

2.02 To prevent inadvertent disclosure of personal health information to unauthorized individuals.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of all employees and contractees of Inscyte and AIM Inc. to ensure that personal health information is secured behind at least two security checkpoints.

4.02 It is the responsibility of the Operations Manager to ensure appropriate physical security checkpoints are implemented and maintained in good working order.

5 DEFINITIONS

5.01 A **Physical Security Checkpoint** is a barrier to entry that requires a key, pass card or access code to open.

5.02 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures.

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.2 Physical Security Access Controls

PS 12.3 Intrusion Detection Controls

PS 12.4 Issuing of Keys, Pass Cards or Access Codes

PS 14.18 Acceptable Use of Remote Network Access

PS 14.19 Acceptable Use of Wireless Network Access

7 PROCEDURE

7.01 None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.1 Physical Isolation of Personal Health Information		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.2 Physical Security Access Controls		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Suitable physical security controls are those that require issuing a personal security token (such as a pass card, key code, or physical key) to an individual allowing him/her to gain access to secured premises, such as:

(a) Electronic keypad door locks
(b) Electronic pass card door locks
(c) Door locks requiring a physical key
(d) Door locks requiring biometric identification

1.02 Wherever possible, electronic security access controls should be implemented that enable automated logging of every use of individual pass cards or access codes.

2 PURPOSE

2.01 To restrict access to personal health information to authorized individuals only.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of AIM's Operations Department to install and maintain physical security access controls and to issue/revoke security tokens to individuals as instructed by the Privacy Officer or Security Officer.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.1 Physical Isolation of Personal Health Information

PS 12.3 Intrusion Detection Controls

PS 12.4 Issuing of Keys, Pass Cards or Access Codes

PS 12.11 Maintaining Entry/Exit Logs

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.3 Intrusion Detection Controls		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 All business premises shall be protected by a commercial grade perimeter alarm system with motion sensors.

1.02 Employees authorized to enter these premises will be issued identity codes and alarm activation/deactivation codes.

1.03 Alarm activation/deactivation codes should be changed on an annual basis.

1.04 Alarm activation/deactivation codes shall be changed in the event of a security breach.

2 PURPOSE

2.01 To detect unauthorized entry to premises (or attempts at unauthorized entry) and alert appropriate staff so that security breaches can be contained and the consequences mitigated.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of AIM's Operations Department to ensure that premises are secured by a perimeter alarm system and that the system is configured appropriately and maintained in good working order.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.12 Intrusion Detection Alarm

PS 12.13 Intrusion Alarm Activation

PS 12.14 Intrusion Alarm De-Activation

PS 12.15 Accidental Activation of Intrusion Alarm

PS 16.3 Actions Following a Breach

7 PROCEDURE

7.01 None

8 REVISION HISTORY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.3 Intrusion Detection Controls		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	
None			

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.4 Issuing of Keys, Pass Cards or Access Codes		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 In general, keys, pass cards, or access codes to physical security checkpoints should only be issued to employees and not to contracted individuals or third parties.

1.02 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 demonstrates that he/she reasonably requires access to general offices outside of normal business hours.
(c) Approval has been given by the Security Officer.

1.03 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 received privacy & security awareness training.
(d) Approval has been given by the Privacy Officer.

1.04 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 received privacy & security awareness training.
(d) Approval has been given by the Privacy Officer.

1.05 Each time an individual is issued a key, pass card or access code the PS 12.7 Log of Individuals Having Access to Premises shall be updated to record the event.

1.06 Each time a key, pass card or access code is revoked or returned the PS 12.7 Log of Individuals Having Access to Premises shall be updated to record the event.

2 PURPOSE

2.01 To control and limit employees' physical access to general offices, secure offices, and computing infrastructure.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.4 Issuing of Keys, Pass Cards or Access Codes		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

4.01 It is the responsibility of the Security Officer to approve/revoke the issue of keys, pass cards, or access codes to general offices.

4.02 It is the responsibility of the Privacy Officer to approve/revoke the issue of keys, pass cards, or access codes to secured offices and to the computing datacenter where personal health information is stored.

4.03 It is the responsibility of the Security Officer to issue/revoke keys, pass cards or access codes and to update the PS 12.7 Log of Individuals Having Access to Premises.

5 DEFINITIONS

5.01 **General Offices** refers to business premises where the storage and use of personal health information is prohibited.

5.02 **Secured Offices** refers to business premises protected by a second physical security checkpoint where the storage and use of personal health information is permitted.

5.03 **The Datacenter** refers to the secured premises protected by a second physical security checkpoint where the computing infrastructure (servers, storage arrays, network routers, back up devices etc.) is located.

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.5 Expiry of Pass Cards and Access Codes

PS 12.7 Log of Individuals Having Access to Premises

PS 12.8 Recovery of Keys, Pass Cards and Access Codes at Termination

PS 12.9 Reporting a Loss of Keys or Pass Cards

PS 12.10 Actions in the Event of Loss of Keys or Pass Cards

PS 12.11 Maintaining Entry/Exit Logs

7 PROCEDURE

7.01 To issue a key, pass card, or access code to General Offices, obtain the approval of the Security Officer and record the event in the PS 12.7 Log of Individuals Having Access to Premises.

7.02 To issue a key, pass card, or access code to Secured Offices or the Datacenter, obtain the approval of the Privacy Officer and record the event in the PS 12.7 Log of Individuals Having Access to Premises.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.5 Expiry of Pass Cards and Access Codes		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Access codes and pass cards to electronic security checkpoints shall expire and be re-issued to affected employees on an annual basis.

1.02 Access codes and pass cards to electronic security checkpoints shall expire and be re-issued to affected employees in the event of a security breach.

2 PURPOSE

2.01 To prevent inadvertent disclosure of access codes that may compromise physical security measures.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that pass cards and access codes are expired and re-issued to affected individuals on an annual basis and following a breach of security.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.7 Log of Individuals Having Access to Premises

PS 16.3 Actions Following a Breach

7 PROCEDURE

7.01 Reset all electronic security checkpoints and re-issue new pass cards and access codes to affected individuals listed in the PS 12.7 Log of Individuals Having Access to Premises.

7.02 Update the PS 12.7 Log of Individuals Having Access to Premises with the new access information.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.6 Secure Storage of Keys and Pass Cards		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Copies of keys to premises and physical pass cards shall be stored in secured offices behind at least two physical security checkpoints.

1.02 Access to keys and the administration of pass cards and access codes shall be limited to designated employees only.

2 PURPOSE

2.01 To safeguard keys and pass cards from theft.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of AIM's Operations Manager to ensure that keys and pass cards are stored in a secure environment.

4.02 It is the responsibility of the Security Officer to designate a limited number of individuals to administer the issuing of keys and administration of pass cards and access codes.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.4 Issuing of Keys, Pass Cards or Access Codes

PS 12.5 Expiry of Pass Cards and Access Codes

PS 12.8 Recovery of Keys, Pass Cards and Access Codes at Termination

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.7 Log of Individuals Having Access to Premises		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A perpetual record shall be maintained of all individuals to whom keys, pass cards or access codes to physical security checkpoints have been issued, revoked and re-issued.

1.02 The **Log of Individuals Having Access to Premises** shall contain the following minimum 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

2 PURPOSE

2.01 To maintain a complete and up-to-date record of all persons who have or at one time had access to general offices, secured offices, the datacenter and other security zones as the case may be.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that the Log of Individuals Having Access to Premises is maintained complete and up-to-date.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.4 Issuing of Keys, Pass Cards or Access Codes

PS 12.5 Expiry of Pass Cards and Access Codes

PS 12.8 Recovery of Keys, Pass Cards and Access Codes at Termination

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.7 Log of Individuals Having Access to Premises		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 12.9 Reporting a Loss of Keys or Pass Cards

PS 12.10 Actions in the Event of Loss of Keys or Pass Cards

PS 3.2 Privacy Document Archives

7 PROCEDURE

7.01 To update the Log of Individuals Having Access to Premises, access the privacy document archives, section: Log of Individuals Having Access to Premises, and open the excel spreadsheet at that location. Make an entry in the table and save the file.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.8 Recovery of Keys, Pass Cards and Access Codes at Termination of Employment		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 At termination of employment or contract, an individual to whom keys, pass cards and/or access codes have been issued shall return these keys and pass cards to the Security Officer and any and all access codes for that individual shall be de-activated.

1.02 The recovery of keys and de-activation of pass cards and access codes for an individual shall be recorded in the PS 12.7 Log of Individuals Having Access to Premises.

2 PURPOSE

2.01 To ensure that the individual who has terminated his/her employment or contract with the company no longer has access to secured premises and that the individual's access codes are no longer in effect.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that keys and pass cards are recovered from individuals who have terminated employment or contract with the company and that access codes for that individual are de-activated.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.11 Actions at Termination of Employment or Contract

PS 12.4 Issuing of Keys, Pass Cards or Access Codes

PS 12.5 Expiry of Pass Cards and Access Codes

PS 12.7 Log of Individuals Having Access to Premises

7 PROCEDURE

7.01 Obtain all copies of keys to business premises in the possession of the individual. Return the keys to secure storage.

7.02 Obtain all pass cards in the possession of the individual and de-activate the pass cards.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.8 Recovery of Keys, Pass Cards and Access Codes at Termination of Employment		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.03 Obtain all access codes (passwords) from the individual or from the PS 12.7 Log of Individuals Having Access to Premises and de-activate the access codes on the affected electronic security checkpoints.

7.03 To update the Log of Individuals Having Access to Premises, access the privacy document archives, section: Log of Individuals Having Access to Premises, and open the excel spreadsheet at that location. Make an entry in the table for each key, pass card and access code that was recovered and de-activated and save the file.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.9 Reporting a Loss of Keys or Pass Cards		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 The loss (or theft) of keys or pass cards shall be reported to the technical support department as soon as the loss or theft is discovered or suspected.

2 PURPOSE

2.01 To alert management as soon as possible about the loss of keys or pass cards that may compromise security measures so that mitigating actions can be taken quickly to prevent a possible breach of security.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of each and every employee or contractee to report the loss or theft of keys and/or pass cards to the technical support department as soon as the loss or theft is discovered or suspected.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.10 Actions in the Event of Loss of Keys or Pass Cards

7 PROCEDURE

7.01 To report lost or stolen keys or pass cards call 416-594-9393 extension 501, or email a message to support@aim.ca. Identify the person whose keys or pass cards were lost or stolen and the time and place that the loss or theft might have occurred.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.10 Actions in the Event of Loss of Keys or Pass Cards or Revocation of Pass Card		Effective:	Nov 7, 2016
		Pages:	1
		Replaces:	Rev 2
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 The access codes pertaining to lost or stolen pass cards shall be de-activated as soon as possible.

1.02 The revoked or lost pass card will be deleted / cancelled from the system, to prohibit fraudulent usage of the card

1.03 The loss of keys or pass cards or revocation of pass cards shall be recorded in the PS 12.7 Log of Individuals Having Access to Premises.

2 PURPOSE

2.01 To mitigate the consequences of a loss or theft or revoked of keys and/or pass cards by de-activating or deleting the access codes for the related security checkpoints as soon as possible.

2.02 To maintain a record of all reported lost or stolen keys and pass cards or any revoked passcards.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to de-activate or delete the access codes pertaining to the lost or stolen or revoked pass card.

4.02 It is the responsibility of the Security Officer to record the loss or theft or revocation of keys or pass cards in the PS 12.7 Log of Individuals Having Access to Premises.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.9 Reporting a Loss of Keys or Pass Cards

PS 12.7 Log of Individuals Having Access to Premises

7 PROCEDURE

7.01 Deactivate the access codes pertaining to the lost or stolen pass card as soon as possible on the related security checkpoints.

7.02 Update the Log of Individuals Having Access to Premises: make an entry in the table for each key and pass card that was reported lost or stolen and de-activated.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.10 Actions in the Event of Loss of Keys or Pass Cards or Revocation of Pass Card		Effective:	Nov 7, 2016
		Pages:	1
		Replaces:	Rev 2
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.11 Maintaining Entry/Exit Logs		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A perpetual **Visitor Log** shall be maintained to record the arrival and departure to/from AIM's **general offices** of persons not employed or contracted by Inscyte Corporation or AIM Inc. who arrive for the purpose of a meeting, consultation, demonstration, etc.

1.02 The **Visitor Log** shall contain the following minimum information:

(a) The name/title of the visitor
(b) The date of arrival
(c) The purpose of the visit
(d) The date of departure

1.03 Postal carriers, couriers, cleaning staff, property managers, delivery persons, or individuals arriving for an interview are not considered to be visitors and do not require entries in the Visitor Log.

1.04 Electronic security checkpoints to **secured offices** and **the Datacenter** should automatically maintain a perpetual log of entry/exit for each use of a pass card or access code.

2 PURPOSE

2.01 To keep a permanent record of visitors to the general offices, and access by authorized personnel to secured offices and the Datacenter.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Office Administrator on duty to update the Visitor Log whenever a third party arrives for a visit and subsequently departs.

4.02 It is the responsibility of the Security Officer to ensure that entry/exit to secured offices and the Datacenter is monitored and logged on a continuous basis.

4.03 It is the responsibility of the Privacy Officer to ensure that the Visitor Log and the Entry/Exit logs to secured offices and the Datacenter are complete and up-to-date.

5 DEFINITIONS

5.01 **General Offices** refers to business premises where the storage and use of personal health information is prohibited.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.11 Maintaining Entry/Exit Logs		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

5.02 **Secured Offices** refers to business premises protected by a second physical security checkpoint where the storage and use of personal health information is permitted.

5.03 **The Datacenter** refers to the secured premises protected by a second physical security checkpoint where the computing infrastructure (servers, storage arrays, network routers, back up devices etc.) is located.

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.1 Physical Isolation of Personal Health Information

PS 12.2 Physical Security Access Controls

7 PROCEDURE

7.01 Whenever a visitor arrives at reception, record the visitor's arrival in the Visitor Log.

7.02 Whenever a visitor departs, record the visitor's departure in the Visitor Log

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.12 Intrusion Detection Alarm		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte Corporation and AIM Inc. shall implement a perimeter intrusion detection alarm for all business premises to trigger an alert in the event of forced or unauthorized entry into the business premises.

1.02 The intrusion detection alarm shall be activated and armed during all periods when the premises are vacant.

1.03 The intrusion detection alarm shall be monitored from an external location having instructions to inform designated members of AIM staff in the event of an alarm.

1.04 Intrusion detection alarm activation/deactivation codes shall be reset at least annually and upon any security breach.

1.05 An employee shall be issued alarm codes and credentials required to cancel a false alarm provided that:

(a) The employee has completed his/her probationary period of employment.
(b) The employee demonstrates that he/she reasonably requires access to general offices outside of normal business hours.
(c) Approval has been given by the Security Officer.

1.06 In the event of termination of contract or employment of an individual to whom alarm activation/deactivation codes and credentials have be issued, those codes and credentials shall be revoked and retired.

2 PURPOSE

2.01 To protect the business premises against unauthorized or forced access and enable appropriate response when an intrusion is detected.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to implement a perimeter intrusion detection alarm system and maintain it in good working order.

4.02 It is the responsibility of the Security Officer to maintain an up-to-date list of AIM personnel to be contacted by the monitoring service in the event that the alarm is triggered, and to provide this list to the monitoring service.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.12 Intrusion Detection Alarm		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

4.03 It is the responsibility of the Security Officer to issue/update alarm activation/deactivation codes and to issue the necessary credentials to employees to cancel a false alarm.

4.05 It is the responsibility of the Security Officer to maintain an accurate, complete and up-to-date log of persons having credentials to cancel a false alarm.

5 DEFINITIONS

5.01 **Business Premises** means the General Offices, Secured Offices and the Datacenter.

5.02 **General Offices** refers to business premises where the storage and use of personal health information is prohibited.

5.03 **Secured Offices** refers to business premises protected by a second physical security checkpoint where the storage and use of personal health information is permitted.

5.04 **The Datacenter** refers to the secured premises protected by a second physical security checkpoint where the computing infrastructure (servers, storage arrays, network routers, back up devices etc.) is located.

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.12 Intrusion Detection Alarm

PS 12.13 Intrusion Alarm Activation

PS 12.14 Intrusion Alarm De-Activation

PS 12.15 Accidental Activation of Intrusion Alarm

PS 12.16 Actions in the Event of an Intrusion Alarm

PS 12.17 Environmental Anomaly Alarms

PS 12.18 Activation of Environmental Alarms

PS 12.19 De-Activation of Environmental Alarms

PS 12.20 Actions in the Event of an Environmental Alarm

7 PROCEDURE

None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.13 Intrusion Alarm Activation		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 The intrusion detection alarm shall be activated whenever the business premises are left vacant.

1.02 The last person to leave the business premises shall activate the intrusion detection alarm.

2 PURPOSE

2.01 To protect the business premises against unauthorized or forced access and enable appropriate response when an intrusion is detected.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the last person leaving secured premises to activate the perimeter intrusion alarm system for those premises.

5 DEFINITIONS

5.01 See definitions of business premises in policy: PS 12.12 Intrusion Detection Alarm

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.12 Intrusion Detection Alarm

PS 12.13 Intrusion Alarm Activation

PS 12.14 Intrusion Alarm De-Activation

PS 12.15 Accidental Activation of Intrusion Alarm

PS 12.16 Actions in the Event of an Intrusion Alarm

PS 12.17 Environmental Anomaly Alarms

PS 12.18 Activation of Environmental Alarms

PS 12.19 De-Activation of Environmental Alarms

PS 12.20 Actions in the Event of an Environmental Alarm

7 PROCEDURE

7.01 To activate the intrusion detection alarm system, locate the alarm panel in your area and enter the activation code, then press “Away”.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.13 Intrusion Alarm Activation		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.14 Intrusion Alarm De-Activation		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 The first authorized person to enter the business premises where the intrusion detection alarm has been activated, shall de-activate the alarm within the allotted time frame to prevent a false alarm from being triggered.

2 PURPOSE

2.01 To protect against triggering a false alarm

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the first authorized person who enters the business premises to de-activate the intrusion detection alarm.

5 DEFINITIONS

5.01 See definitions of business premises in policy: PS 12.12 Intrusion Detection Alarm

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.12 Intrusion Detection Alarm

PS 12.13 Intrusion Alarm Activation

PS 12.14 Intrusion Alarm De-Activation

PS 12.15 Accidental Activation of Intrusion Alarm

PS 12.16 Actions in the Event of an Intrusion Alarm

PS 12.17 Environmental Anomaly Alarms

PS 12.18 Activation of Environmental Alarms

PS 12.19 De-Activation of Environmental Alarms

PS 12.20 Actions in the Event of an Environmental Alarm

7 PROCEDURE

7.01 To de-activate the intrusion detection alarm system, locate the alarm panel in your area and enter the activation code, then press “Off”

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.15 Accidental Activation of Intrusion Alarm		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A person who accidentally triggers the intrusion detection alarm shall immediately contact the monitoring service and provide the required credentials to cancel the alarm.

2 PURPOSE

2.01 To provide a mechanism for cancelling a false alarm.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the person who accidentally triggered the intrusion detection alarm to immediately contact the monitoring service and provide the necessary credentials to cancel the alarm.

5 DEFINITIONS

5.01 See definitions of business premises in policy: PS 12.12 Intrusion Detection Alarm

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.12 Intrusion Detection Alarm

PS 12.13 Intrusion Alarm Activation

PS 12.14 Intrusion Alarm De-Activation

PS 12.15 Accidental Activation of Intrusion Alarm

PS 12.16 Actions in the Event of an Intrusion Alarm

PS 12.17 Environmental Anomaly Alarms

PS 12.18 Activation of Environmental Alarms

PS 12.19 De-Activation of Environmental Alarms

PS 12.20 Actions in the Event of an Environmental Alarm

7 PROCEDURE

7.01 In case of accidental activation of the intrusion alarm the employee must call the alarm company to communicate the accidental activation. You must have the personal ID code ready in order to cancel the accidental activation.

8 REVISION HISTORY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.15 Accidental Activation of Intrusion Alarm		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.16 Actions in the Event of an Intrusion Alarm		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 The following actions shall be taken in the event of an intrusion alarm:

2 PURPOSE

2.01 To respond quickly, effectively and in a coordinated manner in case of a breach of security.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 TBD

5 DEFINITIONS

5.01 TBD

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.12 Intrusion Detection Alarm

PS 12.13 Intrusion Alarm Activation

PS 12.14 Intrusion Alarm De-Activation

PS 12.15 Accidental Activation of Intrusion Alarm

PS 12.16 Actions in the Event of an Intrusion Alarm

PS 12.17 Environmental Anomaly Alarms

PS 12.18 Activation of Environmental Alarms

PS 12.19 De-Activation of Environmental Alarms

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.15 Accidental Activation of Intrusion Alarm		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 12.20 Actions in the Event of an Environmental Alarm

PS 16.3 Actions Following a Breach of Security

7 PROCEDURE

7.01 TBD

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.17 Environmental Anomaly Alarms		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte Corporation and AIM Inc. shall implement environmental anomaly alarm systems in the Datacenter to warn against:

(a) Unacceptable increase in Datacenter temperature
(b) Unacceptable increase in humidity
(c) Smoke and fire detection

2 PURPOSE

2.01 To protect Datacenter components and equipment against damage from elevated operating temperatures, humidity, smoke and fire.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that appropriate environmental alarm systems are implemented and operational at all prescribed times in the Datacenter.

5 DEFINITIONS

5.01 **The Datacenter** refers to the secured premises protected by a second physical security checkpoint where the computing infrastructure (servers, storage arrays, network routers, back up devices etc.) is located.

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.12 Intrusion Detection Alarm

PS 12.13 Intrusion Alarm Activation

PS 12.14 Intrusion Alarm De-Activation

PS 12.15 Accidental Activation of Intrusion Alarm

PS 12.16 Actions in the Event of an Intrusion Alarm

PS 12.17 Environmental Anomaly Alarms

PS 12.18 Activation of Environmental Alarms

PS 12.19 De-Activation of Environmental Alarms

PS 12.20 Actions in the Event of an Environmental Alarm

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.17 Environmental Anomaly Alarms		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.18 Activation of Environmental Alarms		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Environmental Anomaly Alarms shall be activated and operational at all times except for supervised and scheduled outages for maintenance/upgrade purposes.

2 PURPOSE

2.01 To protect Datacenter components and equipment against damage from elevated operating temperatures, humidity, smoke and fire.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that environmental alarms are operational at all times except for scheduled outages.

5 DEFINITIONS

5.01 **The Datacenter** refers to the secured premises protected by a second physical security checkpoint where the computing infrastructure (servers, storage arrays, network routers, back up devices etc.) is located.

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.12 Intrusion Detection Alarm

PS 12.13 Intrusion Alarm Activation

PS 12.14 Intrusion Alarm De-Activation

PS 12.15 Accidental Activation of Intrusion Alarm

PS 12.16 Actions in the Event of an Intrusion Alarm

PS 12.17 Environmental Anomaly Alarms

PS 12.18 Activation of Environmental Alarms

PS 12.19 De-Activation of Environmental Alarms

PS 12.20 Actions in the Event of an Environmental Alarm

7 PROCEDURE

7.01 TBD

8 REVISION HISTORY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.18 Activation of Environmental Alarms		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	
None			

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.19 De-Activation of Environmental Alarms		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 TBD

2 PURPOSE

2.01 TBD

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 TBD

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.12 Intrusion Detection Alarm

PS 12.13 Intrusion Alarm Activation

PS 12.14 Intrusion Alarm De-Activation

PS 12.15 Accidental Activation of Intrusion Alarm

PS 12.16 Actions in the Event of an Intrusion Alarm

PS 12.17 Environmental Anomaly Alarms

PS 12.18 Activation of Environmental Alarms

PS 12.19 De-Activation of Environmental Alarms

PS 12.20 Actions in the Event of an Environmental Alarm

7 PROCEDURE

7.01 TBD

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	12 Physical Security		
PS 12.20 Actions in the Event of an Environmental Alarm		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 The following actions shall be taken in the event of an environmental alarm:

2 PURPOSE

2.01 To respond quickly, effectively and in a coordinated manner in case of an environmental anomaly to mitigate the extent of damage from excessive temperatures, humidity, smoke or fire.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.12 Intrusion Detection Alarm

PS 12.13 Intrusion Alarm Activation

PS 12.14 Intrusion Alarm De-Activation

PS 12.15 Accidental Activation of Intrusion Alarm

PS 12.16 Actions in the Event of an Intrusion Alarm

PS 12.17 Environmental Anomaly Alarms

PS 12.18 Activation of Environmental Alarms

PS 12.19 De-Activation of Environmental Alarms

PS 12.20 Actions in the Event of an Environmental Alarm

7 PROCEDURE

7.01 TBD

8 REVISION HISTORY

None

13 Retention, Storage, Transfer, and Disposal of Personal Health Information

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.1 Appropriate Retention Periods for PHI		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal Health Information shall only be retained for as long as permitted under the **Statement of Retention** for the data holding in question.

1.02 In the event that the personal health information does not have a specified Statement of Retention then the retention period shall be the **minimum time period** required to perform the work for which the personal health information is required.

1.03 Upon expiry of the retention period for a holding of personal health information , the personal health information shall be **disposed of forthwith** in accordance with the policies and procedures for the disposal of personal health information.

2 PURPOSE

2.01 To ensure that personal health information is retained for the minimum required period.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of each and every employee and contractee of AIM to retain personal health information for the minimum required time period and dispose of the information thereafter in the appropriate manner.

4.02 It is the responsibility of the Privacy Officer to ensure that holdings of personal health information are only retained in accordance with the Statements of Retention for each data holding.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 4.10 Maintaining Statements of Retention

PS 13.13 Disposal of PHI – Paper Records

PS 13.14 Disposal of PHI – Portable Media

PS 13.15 Disposal of PHI – Files/Database Systems

7 PROCEDURE

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.1 Appropriate Retention Periods for PHI		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.2 Storage of PHI – Paper Records		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal Health Information in printed form shall be stored in secured offices behind at least two physical security checkpoints.

1.02 Personal Health Information in printed form should further be stored in file cabinets secured by a lock and key.

1.03 Personal Health Information in printed form should be organized into folder or folios that clearly identify the type and source of the information.

2 PURPOSE

2.01 To safeguard personal health information from theft and inadvertent disclosure.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of every individual working with personal health information in printed form to ensure that the information is stored in accordance with this policy.

4.02 It is the responsibility of the Privacy Officer to ensure that personal health information in printed form is stored with the required safeguards in place.

5 DEFINITIONS

5.01 See definition of personal health information in policy 0 PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.1 Physical Isolation of Personal Health Information

PS 13.3 Storage of PHI – Portable Media

PS 13.4 Storage of PHI – Mobile Devices

PS 13.5 Storage of PHI – Email Archives

PS 13.6 Storage of PHI – File/Database Systems

PS 4.2 Collection of PHI – Paper Records

7 PROCEDURE

7.01 None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.2 Storage of PHI – Paper Records		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.3 Storage of PHI – Portable Media		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal health information stored on portable media shall be stored in secured offices behind at least two physical security checkpoints.

1.02 The portable media should further be stored in file cabinets secured by a lock and key.

1.03 Files of personal health information stored on portable media should be safeguarded by applying the following precautions

(a) The files on the portable media that contain personal health information should be encrypted and password protected, or
(b) Access to the portable memory device itself should be password protected.

2 PURPOSE

2.01 To safeguard personal health information from theft and inadvertent disclosure.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of every individual working with personal health information on portable media to ensure that the information is stored in accordance with this policy.

4.02 It is the responsibility of the Privacy Officer to ensure that personal health information in on portable is stored with the required safeguards in place.

5 DEFINITIONS

5.01 **Portable Media** means diskettes, tapes, CDs, DVDs, USB keys and other portable storage media.

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.1 Physical Isolation of Personal Health Information

PS 13.2 Storage of PHI – Paper Records

PS 13.4 Storage of PHI – Mobile Devices

PS 13.5 Storage of PHI – Email Archives

PS 13.6 Storage of PHI – File/Database Systems

PS 4.3 Collection of PHI – Portable Media

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.3 Storage of PHI – Portable Media		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 14.6 Requirements for Passwords

7 PROCEDURE

7.01 To encrypt and password protect a file (or set of files) it is permissible to use a commercial software tool such as PK-Zip or WinZip.

7.02 The password used to lock the file(s) must not be noted or contained with the portable media itself. The password should be communicated to the receiver by telephone or by an email message.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.4 Storage of PHI – Mobile Devices		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal health information shall not be stored on mobile devices.

2 PURPOSE

2.01 To safeguard personal health information from theft and inadvertent disclosure.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of every individual to ensure that no personal health information is retained on mobile devices.

4.02 It is the responsibility of the Security Officer to periodically audit the use of mobile devices to monitor compliance with this policy.

5 DEFINITIONS

5.01 **Mobile Devices** means portable computing devices that can be used alone to store, retrieve and manipulate data, such as laptops, notebooks, tablets, PDAs, and smart phones.

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.1 Physical Isolation of Personal Health Information

PS 13.2 Storage of PHI – Paper Records

PS 13.3 Storage of PHI – Portable Media

PS 13.5 Storage of PHI – Email Archives

PS 13.6 Storage of PHI – File/Database Systems

PS 4.4 Collection of PHI – Mobile Devices

PS 14.5 Requirements for Access Accounts

PS 14.6 Requirements for Passwords

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.4 Storage of PHI – Mobile Devices		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.5 Storage of PHI – Email Archives		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal health information shall not be stored in email messages or message archives on email clients or email servers.

1.02 Any personal health information received via email should be saved to a location on a server that is part of the secure PHI network and the email message should be deleted both on the email client and the email server forthwith.

2 PURPOSE

2.01 To prevent personal health information from unauthorized and/or inadvertent disclosure.

2.02 To account for the fact that Email systems are inherently dynamic and volatile and cannot be adequately controlled in terms of restricting the content of information sent/received or safeguarding such information from unauthorized access.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of every individual to ensure that their email client does not contain archived messages containing personal health information or file attachments that contain personal health information.

4.02 It is the responsibility of the Operations Manager to ensure that email servers do not contain messages containing personal health information or file attachments that contain personal health information.

5 DEFINITIONS

5.01 **Email Archives** refers to messages and file attachments stored on an email client or on an email server.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.4 Storage of PHI – Mobile Devices		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

6 REFERENCES and related POLICIES & PROCEDURES

PS 13.2 Storage of PHI – Paper Records

PS 13.3 Storage of PHI – Portable Media

PS 13.4 Storage of PHI – Mobile Devices

PS 13.6 Storage of PHI – File/Database Systems

PS 4.5 Collection of PHI – Email

PS 14.1 Isolation of PHI Computers and Networks

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.6 Storage of PHI – File/Database Systems		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal health information stored in computer file systems or database management systems shall only be stored on computers and/or storage arrays physically located behind at least two security checkpoints and accessible through a secure network dedicated to personal health information and not the general business network.

1.02 Access to the file systems or database management systems that contain personal health information shall require authenticating a unique user ID and password combination (unique for each person granted access rights).

1.03 All attempts to access file systems or database management systems that contain personal health information should be logged and audited.

1.04 It is not necessary to encrypt files systems or databases containing personal health information provided that policy 1.01 is in force.

2 PURPOSE

2.01 To safeguard personal health information from theft and inadvertent disclosure.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that proper precautions are in place for the storage of personal health information in computer files systems or database management systems.

4.02 It is the responsibility of the Technical Service Department to ensure that security controls required to protect personal health information in computer files systems of databases are in place and functional at all times.

5 DEFINITIONS

5.01 **File/Database Systems** means organized/managed digital files systems on a mobile device, desktop or server. Examples include:

(a) Database Management System (Oracle, SQL Server, MySQL etc.)
(b) Document Management Systems (Source Safe, SharePoint, etc.)
(c) Email Servers
(d) Operating System File Systems

6 REFERENCES and related POLICIES & PROCEDURES

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.6 Storage of PHI – File/Database Systems		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 12.1 Physical Isolation of Personal Health Information

PS 14.1 Isolation of PHI Computers and Networks

PS 13.2 Storage of PHI – Paper Records

PS 13.3 Storage of PHI – Portable Media

PS 13.4 Storage of PHI – Mobile Devices

PS 13.5 Storage of PHI – Email Archives

PS 14.1 Isolation of PHI Computers and Networks

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.7 Transfer of PHI – Paper Records		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 If personal health information is to be transferred from one location to another in paper-based format (clinical report forms, letters, lab reports, etc.) the following precautions shall be taken during the transfer process:

(a) The paper-based records shall be enclosed in a sealed envelope or box.
(b) The packages shall identify the individual recipient and sender of the information.
(c) The package shall identify the date when the records were sealed.
(d) The package should be labeled to clearly describe that it contains PHI and the nature of the content. For example: "PHI: Inscyte CytoBase Lab Results for Manual Correction".

1.02 Paper-based records may not be transported by federal post. Paper-based records shall be transported via commercial bonded courier, by couriers of participating healthcare custodians (laboratories) of CytoBase, or by the designated staff of either the sender or recipient.

1.03 All transfers of personal health information in paper format shall be recorded in a perpetual **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)

2 PURPOSE

2.01 To safeguard personal health information from inadvertent disclosure, theft or loss during the transfer process.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure appropriate safeguards are implemented during the transfer of personal health information in paper-based format.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.7 Transfer of PHI – Paper Records		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 13.2 Storage of PHI – Paper Records

PS 4.2 Collection of PHI – Paper Records

PS 13.8 Transfer of PHI – Portable Media

PS 13.9 Transfer of PHI – Mobile Devices

PS 13.10 Transfer of PHI – Email

PS 13.11 Transfer of PHI – Network Transfer

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.8 Transfer of PHI – Portable Media		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 If personal health information is to be transferred from one location to another using portable media (see definition below) the following precautions shall be taken during the transfer process:

(a) The files on the portable media that contain personal health information shall be encrypted and password protected, and/or
(b) The portable memory device itself shall be password protected.
(c) The portable media should be labeled to clearly describe that it contains PHI and the nature of the content. For example: "PHI: Inscyte CytoBase Lab Results for Manual Correction".

1.02 Portable media may not be transported by federal post. Portable media shall be transported via commercial courier or by the designated staff of either the sender or recipient.

1.03 Portable media containing PHI should not be left unattended and publicly visible during the transfer process.

2 PURPOSE

2.01 To safeguard personal health information from theft or loss during the transfer process.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure appropriate safeguards are implemented during transfers of personal health information using portable media.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

5.02 **Portable Media** means diskettes, tapes, CDs, DVDs, USB keys and other portable storage media.

6 REFERENCES and related POLICIES & PROCEDURES

PS 13.3 Storage of PHI – Portable Media

PS 13.7 Transfer of PHI – Paper Records

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.8 Transfer of PHI – Portable Media		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 13.9 Transfer of PHI – Mobile Devices

PS 13.10 Transfer of PHI – Email

PS 13.11 Transfer of PHI – Network Transfer

PS 14.5 Requirements for Access Accounts

PS 14.6 Requirements for Passwords

7 PROCEDURE

7.01 To encrypt and password protect a file (or set of files) it is permissible to use a commercial software tool such as PK-Zip or WinZip.

7.02 The password used to lock the file(s) must not be noted or contained with the portable media itself. The password should be communicated to the receiver by telephone or by an email message.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.9 Transfer of PHI – Mobile Devices		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Mobile devices shall not be used for the transfer of personal health information.

2 PURPOSE

2.01 To safeguard personal health information from inadvertent disclosure, theft or loss during the transfer process.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its Agent.

4 RESPONSIBILITY

4.01 It is the responsibility of every individual to ensure that no personal health information is retained on mobile devices.

4.02 It is the responsibility of the Security Officer to periodically audit the use of mobile devices to monitor compliance with this policy.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

5.02 **Mobile Devices** means portable computing devices that can be used alone for the storage, retrieval and manipulation of data, such as laptops, notebooks, tablets, PDAs, and smart phones.

6 REFERENCES and related POLICIES & PROCEDURES

PS 13.4 Storage of PHI – Mobile Devices

PS 13.7 Transfer of PHI – Paper Records

PS 13.8 Transfer of PHI – Portable Media

PS 13.10 Transfer of PHI – Email

PS 13.11 Transfer of PHI – Network Transfer

PS 14.5 Requirements for Access Accounts

PS 14.6 Requirements for Passwords

7 PROCEDURE

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.9 Transfer of PHI – Mobile Devices		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.10 Transfer of PHI – Email		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal health information should not be transferred from one location to another using email unless there are no reasonable alternative modes of transfer

1.02 If email transfer is necessitated the personal health information shall be contained in contained in a file attachment only and the file shall be encrypted and password protected.

1.02 The password to unlock an encrypted file attachment shall not be communicated to the recipient using email. It should be communicated to the recipient personally by telephone allowing the sender to verify the recipient's identity.

1.03 Any personal health information received via email or an email attachment should be saved to a location on a server that is part of the secure PHI network and the email message should be deleted from the email client and the email server forthwith.

2 PURPOSE

2.01 To safeguard personal health information from inadvertent disclosure, theft or loss during the transfer process.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure appropriate safeguards are implemented during the transfer of personal health information via email.

4.02 It is the responsibility of every individual handling PHI to ensure that email transfers of PHI comply with this policy but, in any event, are avoided whenever possible.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 4.5 Collection of PHI – Email

PS 13.5 Storage of PHI – Email Archives

PS 13.7 Transfer of PHI – Paper Records

PS 13.8 Transfer of PHI – Portable Media

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.10 Transfer of PHI – Email		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 13.9 Transfer of PHI – Mobile Devices

PS 13.11 Transfer of PHI – Network Transfer

PS 14.1 Isolation of PHI Computers and Networks

PS 14.6 Requirements for Passwords

7 PROCEDURE

7.01 To encrypt and password protect a file (or set of files) it is permissible to use a commercial software tool such as PK-Zip or WinZip.

7.02 The password used to lock the file(s) must not be noted or contained within the email message. The password should be communicated to the receiver by telephone or other means.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.11 Transfer of PHI – Network Transfer		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 If personal health information is to be transferred from one location to another using a computer network the following precautions shall be taken during the transfer process:

(a) The network connection between sending and receiving systems shall be encrypted using a self-managed or third-party public key infrastructure (PKI) mechanism.
(b) Access to the network shall require authentication of a unique account name and password combination (user login).

1.02 In addition, when possible, individual files (or messages) being transferred should also be encrypted even if the network itself is encrypted (i.e. use double encryption).

2 PURPOSE

2.01 To safeguard personal health information from inadvertent disclosure or loss during the collection process.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure appropriate safeguards are implemented during the transfer of personal health information over a computer network.

4.02 It is the responsibility of every individual handling PHI to ensure that network transfers of PHI comply with this policy.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 13.7 Transfer of PHI – Paper Records

PS 13.8 Transfer of PHI – Portable Media

PS 13.9 Transfer of PHI – Mobile Devices

PS 13.10 Transfer of PHI – Email

7 PROCEDURE

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.11 Transfer of PHI – Network Transfer		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.01 Network transfer of personal health information should be used when the collection process is on-going or repetitive.

7.02 Acceptable encryption strength is 1024+ bits.

7.03 If collection of PHI is performed using a network application (such as a web application) use a third-party server security certificate on the application server to encrypt and secure the network connection (e.g. VeriSign)

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.12 Log of PHI Transfers		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A perpetual **Log of PHI Transfers** shall be maintained to document the transfers of personal health information from/to Inscyte Corporation and third parties.

1.02 The **Log of PHI Transfers** shall contain the following minimum information:

(a) The date of the transfer
(b) The name of the sender
(c) The name of the recipient
(d) How the transfer was performed (paper, portable media, mobile device, email, or network)
(e) Name of courier and waybill number (if appropriate)
(f) Purpose of the transfer
(g) A summary of the information transferred

1.03 In the event that transfers of personal health information occur using an automated mechanism, that mechanism shall include:

(a) The automated compilation of a transfer audit log in accordance with policy item 1.02 above.
(b) Creating an audit entry for each person affected by the transfer describing what information was transferred (disclosed), to whom, and at what date/time.

2 PURPOSE

2.01 To maintain a complete record of privacy complaints received and the actions taken to investigate and resolve each complaint.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that the Log of PHI Transfers is complete and up-to-date.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 13.7 Transfer of PHI – Paper Records

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.12 Log of PHI Transfers		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 13.8 Transfer of PHI – Portable Media

PS 13.9 Transfer of PHI – Mobile Devices

PS 13.10 Transfer of PHI – Email

PS 13.11 Transfer of PHI – Network Transfer

7 PROCEDURE

7.01 The manual Log of PHI Transfers is found in AIM's PS 3.2 Privacy Document Archives in section – Log of PHI Transfers.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.13 Disposal of PHI – Paper Records		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Printed documents containing personal health information shall be disposed of by cross-cut shredding, pulverization or incineration of the documents.

1.02 If a third-party service is engaged for the shredding or destruction of paper records, the third party shall be 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.

1.03 Printed documents containing personal health information shall not be disposed of in waste baskets, re-cycling bins, or any other normal waste disposal methods.

2 PURPOSE

2.01 To ensure that personal information on paper records is disposed of in a manner rendering it reasonably impossible to recover or reconstruct the information.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that appropriate mechanisms are in place for the disposal and destruction of paper records containing personal health information.

4.02 It the responsibility of each and every staff member and contractee of AIM to use the mechanisms in place for the disposal and destruction of personal health information in paper form.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 13.13 Disposal of PHI – Paper Records

PS 13.14 Disposal of PHI – Portable Media

PS 13.15 Disposal of PHI – Files/Database Systems

7 PROCEDURE

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.13 Disposal of PHI – Paper Records		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.01 AIM Inc. offices premises are outfitted with locked "ShredEx" document disposal cabinets. The documents dropped into these cabinets are destroyed on a scheduled basis by a third party document management company.

7.02 To dispose of documents containing personal health information, simply drop the documents into one of the "ShredEx" cabinets.

7.03 In general, once a document is dropped into one of these cabinets it cannot be retrieved. The keys to the cabinets are maintained by the Privacy Officer (or delegate).

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.14 Disposal of PHI – Portable Media		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Personal health information recorded on portable media shall be disposed of by rendering the media unusable and discarding the media, or

1.02 If the portable media are to be re-used by the organization authorized to store personal health information, by deleting the files using a method that renders the files non-recoverable.

2 PURPOSE

2.01 To ensure that personal information on portable media is disposed of in a manner rendering it reasonably impossible to recover or reconstruct the information.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that appropriate mechanisms are in place for the disposal and/or destruction of portable media containing personal health information.

4.02 It the responsibility of each and every staff member and contractee of AIM to use the mechanisms in place for the disposal and/or destruction of personal health information on portable media.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

5.02 **Portable Media** means diskettes, tapes, CDs, DVDs, USB keys and other portable storage media.

6 REFERENCES and related POLICIES & PROCEDURES

PS 13.13 Disposal of PHI – Paper Records

PS 13.15 Disposal of PHI – Files/Database Systems

PS 13.16 Deleting Files from Re-usable Storage Devices

PS 13.17 Destruction of Internal Computer Disk Drives

PS 13.18 Destruction of Diskettes, CDs and DVDs

PS 13.19 Destruction of Tapes

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.14 Disposal of PHI – Portable Media		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 13.20 Destruction of Flash Memory Devices (USB Keys)

7 PROCEDURE

7.01 If the media are to be rendered unusable and discarded, destroy the media in accordance with policies PS 13.18 Destruction of Diskettes, CDs and DVDs or PS 13.20 Destruction of Flash Memory Devices (USB Keys).

7.02 If the media re to be retained by the organization for re-use, delete the files of personal health information that are no longer needed in accordance with policy PS 13.16 Deleting Files from Re-usable Storage Devices.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.15 Disposal of PHI – Files/Database Systems		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Records of personal health information shall be deleted from file/database systems when these records are no longer required or when the retention period for these records has expired.

1.02 Deleting records from a managed file/database system does not ensure the destruction of the records since the file/database system will usually include a mechanism to restore the deleted data from cache(s) of deleted records. In this case, the records shall also be deleted from the cache(s) so that they become unrecoverable.

1.03 If a file/database system is to be decommissioned entirely, all component files of the file/database management system shall be deleted in accordance with policy PS 13.16 Deleting Files from Re-usable Storage Devices, or

1.04 If no longer required, the physical storage devices of the file/database management system (hard disks etc.) shall be destroyed in accordance with policy PS 13.17 Destruction of Internal Computer Disk Drives.

2 PURPOSE

2.01 To ensure that personal information stored in file/database systems is disposed of in a manner rendering it reasonably impossible to recover or reconstruct the information.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that appropriate mechanisms are in place for the disposal of personal health information contained in a managed file/database system.

4.02 It the responsibility of each and every staff member and contractee of AIM to use the mechanisms in place for the disposal of personal health information in managed file/database systems.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.15 Disposal of PHI – Files/Database Systems		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

5.01 **File/Database Systems** means organized/managed digital files systems on a mobile device, desktop or server. Examples include:

(a) Database Management System (Oracle, SQL Server, MySQL etc.)
(b) Document Management Systems (Source Safe, SharePoint, etc.)
(c) Email Servers
(d) Operating System File Systems

6 REFERENCES and related POLICIES & PROCEDURES

PS 13.13 Disposal of PHI – Paper Records

PS 13.14 Disposal of PHI – Portable Media

PS 13.17 Destruction of Internal Computer Disk Drives

PS 13.18 Destruction of Diskettes, CDs and DVDs

PS 13.19 Destruction of Tapes

PS 13.20 Destruction of Flash Memory Devices (USB Keys)

7 PROCEDURE

7.01 If selected records or personal health information are no longer required, delete these records from the file/database system using the data management tools available.

7.02 If all records in a file/database system are no longer required, decommission the file/database system by securely deleting all related files from the storage media in accordance with policy PS 13.16 Deleting Files from Re-usable Storage Devices.

7.03 If the storage devices are no longer required, permanently dispose of the storage devices in accordance with policies:

PS 13.17 Destruction of Internal Computer Disk Drives

PS 13.18 Destruction of Diskettes, CDs and DVDs

PS 13.19 Destruction of Tapes

PS 13.20 Destruction of Flash Memory Devices (USB Keys)

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.16 Deleting Files from Re-usable Storage Devices		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Computer files containing personal health information stored on re-usable storage media shall be deleted when no longer required, or when the retention period for personal health information has expired.

1.02 Computer files containing personal health information stored on re-usable storage media shall be deleted using a mechanism that prevents the files from being recovered or restored.

2 PURPOSE

2.01 To ensure that computer files containing personal health information are deleted in a manner rendering it reasonably impossible to recover or reconstruct the files.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that appropriate mechanisms are in place for safely deleting files of personal health information from re-usable storage devices.

4.02 It the responsibility of each and every staff member and contractee of AIM to use the mechanisms in place to safely delete files of personal health information from re-usable storage devices when required.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

5.02 **Re-usable Storage Devices** means re-writeable diskettes, CDs, DVDs, USB keys or internal storage drives on printers, faxes, mobile devices, etc.

5.03 **Mobile Devices** means portable computing devices such as laptops, notebooks, tablets, PDAs, smart phones etc.

6 REFERENCES and related POLICIES & PROCEDURES

PS 13.14 Disposal of PHI – Portable Media

PS 13.15 Disposal of PHI – Files/Database Systems

PS 13.17 Destruction of Internal Computer Disk Drives

PS 13.18 Destruction of Diskettes, CDs and DVDs

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.16 Deleting Files from Re-usable Storage Devices		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 13.19 Destruction of Tapes

PS 13.20 Destruction of Flash Memory Devices (USB Keys)

7 PROCEDURE

7.01 Method 1: to permanently delete files from a computer drive use commercial file shredding software such as “Eraser” or “XL Delete”. These tools employ algorithmic methods that delete files and over-write the disk space allocated to those files with random patterns that prevent restoration or recovery of the data.

7.02 Method 2: reformat computer disk drives to wipe data and re-create new file allocation tables. This is not as effective as method 1 but makes it very difficult to restore deleted files.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.17 Destruction of Internal Computer Disk Drives		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 When internal computer storage drives that may contain personal health information are to be replaced or decommissioned, the drives shall be physically destroyed in a manner that renders the drives unusable and prevents reading of any data from the drives.

1.02 Computer storage drives that may contain personal health information shall not be sent out for repair or recycling.

2 PURPOSE

2.01 To ensure that computer drives that contain personal health information are destroyed of in a manner rendering it reasonably impossible to recover or reconstruct the information.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that appropriate mechanisms are in place for safely destroying computer disk drives.

4.02 It the responsibility of each and every staff member and contractee of AIM to use the mechanisms in place to safely destroy computer disk drives when required.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 13.18 Destruction of Diskettes, CDs and DVDs

PS 13.19 Destruction of Tapes

PS 13.20 Destruction of Flash Memory Devices (USB Keys)

7 PROCEDURE

7.01 Remove the disk(s) from the computer housing.

7.02 Open the disk chassis and remove the platters, by force, if necessary.

7.03 Deform the platters to destroy alignment.

8 REVISION HISTORY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.17 Destruction of Internal Computer Disk Drives		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	
None			

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.18 Destruction of Diskettes, CDs and DVDs		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 When diskettes, CDs or DVDs that may contain personal health information are no longer required, the diskettes, CDs and/or DVDs shall be physically destroyed in manner that makes them unusable and prevents reading of the data on these media.

1.02 Diskettes, CDs or DVDs that may contain personal health information shall not be recycled.

2 PURPOSE

2.01 To ensure that diskettes, CDs and/or DVDs containing personal information are destroyed of in a manner rendering it reasonably impossible to recover or reconstruct the information.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that appropriate mechanisms are in place for safely destroying diskettes, CDs or DVDs.

4.02 It the responsibility of each and every staff member and contractee of AIM to use the mechanisms in place to safely destroy diskettes, CDs or DVDs when required.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 13.17 Destruction of Internal Computer Disk Drives

PS 13.19 Destruction of Tapes

PS 13.20 Destruction of Flash Memory Devices (USB Keys)

7 PROCEDURE

7.01 Remove or black out any information printed on the diskette, CD or DVD that describes the contents, author, owner, sender or recipient of the data.

7.02 Make deep scratches into the optical surface of the CD or DVD. Cut the media into at least five pieces and deform the pieces.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.18 Destruction of Diskettes, CDs and DVDs		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.03 Dispose of the pieces in at least two separate disposal locations.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.19 Destruction of Tapes		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 When magnetic tapes that may contain personal health information are no longer required, the tapes shall be physically destroyed in manner that makes them unusable and prevents reading of the data.

1.02 Magnetic tapes that may contain personal health information shall not be recycled.

2 PURPOSE

2.01 To ensure that magnetic tapes containing personal information are destroyed of in a manner rendering it reasonably impossible to recover or reconstruct the information.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that appropriate mechanisms are in place for safely destroying magnetic tapes.

4.02 It the responsibility of each and every staff member and contractee of AIM to use the mechanisms in place to safely destroy magnetic tapes when required.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 13.17 Destruction of Internal Computer Disk Drives

PS 13.18 Destruction of Diskettes, CDs and DVDs

PS 13.20 Destruction of Flash Memory Devices (USB Keys)

7 PROCEDURE

7.01 Remove or black out any information printed on the tape housing that describes the contents, author, owner, sender or recipient of the data.

7.02 Break apart the tape housing and pull out the tape. Shred or cut the tape into at least twenty pieces.

7.03 Dispose of the pieces in at least two separate disposal locations.

8 REVISION HISTORY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.19 Destruction of Tapes		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	
None			

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.20 Destruction of Flash Memory Devices (USB Keys)		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 When electronic memory devices such as USB keys that may contain personal health information are no longer required, the electronic memory devices shall be physically destroyed in manner that makes them unusable and prevents reading of the data.

1.02 Electronic memory devices such as USB keys that may contain personal health information shall not be sent out for repair or recycling.

2 PURPOSE

2.01 To ensure that electronic memory devices such as USB keys containing personal information are destroyed of in a manner rendering it reasonably impossible to recover or reconstruct the information.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that appropriate mechanisms are in place for safely destroying electronic memory devices such as USB keys.

4.02 It the responsibility of each and every staff member and contractee of AIM to use the mechanisms in place to safely destroy electronic memory devices when require

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

PS 13.17 Destruction of Internal Computer Disk Drives

PS 13.18 Destruction of Diskettes, CDs and DVDs

PS 13.19 Destruction of Tapes

7 PROCEDURE

7.01 Crush and/or break apart the electronic memory device or USB key by using a hammer or other device.

8 REVISION HISTORY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	13 Retention, Storage, Transfer, and Disposal of Personal Health Information		
PS 13.20 Destruction of Flash Memory Devices (USB Keys)		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	
None			

14 Information Security

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.1 Isolation of PHI Computers and Networks		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 The organization's computing in infrastructure shall be divided into two secure segments: the business network and the PHI network.

1.02 Personal health information shall not be persisted on computers that are connected to the business network, but only on computers connected to the PHI network.

1.03 Computers and peripheral devices connected to the PHI network shall be located behind at least two physical security checkpoints.

1.04 Access to the PHI network shall require a unique account/password combination for each authorized individual.

1.05 Authorization to issue an account/password to an individual to access the PHI network shall require approval by the Privacy Officer.

2 PURPOSE

2.01 To secure personal health information from unauthorized access.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that the computing infrastructure is divided and maintained as two networks: the general business network and the PHI network.

4.02 It is the responsibility of the Security Officer to ensure that both networks are maintained and managed in a manner that prevents the unauthorized access to the PHI network and detects attempts at unauthorized access.

4.03 It is the responsibility of the Security Officer to ensure that access accounts/passwords are administered in the appropriate manner, monitored and audited.

4.04 It is the responsibility of the Privacy Officer to approve individual access accounts to the PHI network, its applications, and data holdings.

5 DEFINITIONS

5.01 See definition of personal health information in policy PS 1.1 Existence of Policies and Procedures

6 REFERENCES and related POLICIES & PROCEDURES

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.1 Isolation of PHI Computers and Networks		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 14.2 Issuing Network Accounts and Passwords

PS 14.3 Issuing Application Specific Accounts and Passwords

PS 14.4 Issuing Database System Accounts and Passwords

PS 14.5 Requirements for Access Accounts

PS 14.6 Requirements for Passwords

PS 14.7 Mandatory Password Expiry

PS 14.8 Limits on Password Re-Use

PS 14.9 Log of Accounts Having Access to PHI

PS 14.10 Decommissioning of Accounts upon Termination

PS 14.11 Maintaining Information Access Audit Logs

PS 14.12 Failed Authentication Account Lockout

7 PROCEDURE

None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.2 Issuing Network Accounts and Passwords		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Network accounts/passwords to access the PHI network shall only be granted to individuals who have a genuine need to access the PHI network and not to all staff, and provided that:

(a) The individual is an employee of Inscyte Corporation or AIM Inc.
(b) The individual has executed a Confidentiality Agreement.
(c) The individual has received privacy and security awareness training.

1.02 Accounts to access the PHI network shall be enabled only after approval of the Privacy Officer has been obtained.

1.03 Account names and passwords shall be issued in accordance with the policies governing name/password composition, password expiry, and re-use.

1.04 Issuance and revocation of accounts to access the PHI network shall be recorded in the PS 14.9 Log of Accounts Having Access to PHI.

2 PURPOSE

2.01 To secure personal health information from unauthorized access and maintain an accurate log of individuals having access to PHI.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that access accounts/passwords are administered in the appropriate manner, monitored and audited.

4.02 It is the responsibility of the Privacy Officer to approve individual access accounts to the PHI network, its applications, and data holdings.

5 DEFINITIONS

5.01 A **Network Account** is an operating system level account that enables a user to access a computer, its file system and network services.

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.1 Isolation of PHI Computers and Networks

PS 14.3 Issuing Application Specific Accounts and Passwords

PS 14.4 Issuing Database System Accounts and Passwords

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.2 Issuing Network Accounts and Passwords		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 14.5 Requirements for Access Accounts

PS 14.6 Requirements for Passwords

PS 14.7 Mandatory Password Expiry

PS 14.8 Limits on Password Re-Use

PS 14.9 Log of Accounts Having Access to PHI

PS 14.10 Decommissioning of Accounts upon Termination

PS 14.11 Maintaining Information Access Audit Logs

PS 14.12 Failed Authentication Account Lockout

7 PROCEDURE

7.01 Network accounts are given to users with first name initial plus full last name (i.e. John Doe; jdoe@aim.ca). A temporary password is assigned to new user accounts and the owner must change the temporary password at first login as per PS 14.6 Requirements for Passwords. The network rights are dictated by department managers.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.3 Issuing Application Specific Accounts and Passwords		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Applications used to administer and manage specific data holdings on the PHI network shall require unique application specific accounts and passwords (beyond that required to access the PHI network itself) to be issued to individual users of the application.

1.02 Accounts to use specific applications on the PHI network shall only be granted to individuals who have a genuine need to use these applications and not to all staff, and provided that:

(a) The individual is an employee of Inscyte Corporation or AIM Inc.
(b) The individual has executed a Confidentiality Agreement.
(c) The individual has received privacy and security awareness training.

1.03 Accounts to use specific applications shall be enabled only after approval of the Privacy Officer has been obtained.

1.04 Application access account names and passwords shall be issued in accordance with the policies governing name/password composition, password expiry, and re-use.

1.05 Issuance and revocation of application specific accounts shall be recorded in the PS 14.9 Log of Accounts Having Access to PHI.

2 PURPOSE

2.01 To secure personal health information from unauthorized access and use and maintain an accurate log of individuals having access to specific applications in respect of PHI.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that application specific access accounts/passwords are administered in the appropriate manner, monitored and audited.

4.02 It is the responsibility of the Privacy Officer to approve application specific access accounts.

5 DEFINITIONS

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.3 Issuing Application Specific Accounts and Passwords		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

5.01 An **Application-Specific Account** is a username and password combination that is authenticated by an application itself, and not by the network/computer on which the application executes nor by a back-end database related to that application.

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.1 Isolation of PHI Computers and Networks

PS 14.2 Issuing Network Accounts and Passwords

PS 14.4 Issuing Database System Accounts and Passwords

PS 14.5 Requirements for Access Accounts

PS 14.6 Requirements for Passwords

PS 14.7 Mandatory Password Expiry

PS 14.8 Limits on Password Re-Use

PS 14.9 Log of Accounts Having Access to PHI

PS 14.10 Decommissioning of Accounts upon Termination

PS 14.11 Maintaining Information Access Audit Logs

PS 14.12 Failed Authentication Account Lockout

7 PROCEDURE

7.01 Application specific accounts are only given to users as deemed necessary. Department managers will determine which application accounts will be given to the user. The user will be assigned a temporary password and must change it at first login.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.4 Issuing Database System Accounts and Passwords		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Whenever possible, accounts that enable access to database systems containing personal health information should be obfuscated by employing a "pooled alias login" mechanism whereby each individual user is authenticated by an application using an application-specific account name/password and not an actual database account/password.

1.02 Accounts to access database systems containing personal health information at the administrator level shall only be granted to a limited number of individuals designated as "database administrators" and only providing that:

(a) The individual is an employee of Inscyte Corporation or AIM Inc.
(b) The individual has executed a Confidentiality Agreement.
(c) The individual has received privacy and security awareness training.

1.03 Accounts to access database systems shall be enabled only after approval of the Privacy Officer has been obtained.

1.04 Database access account names and passwords shall be issued in accordance with the policies governing name/password composition, password expiry, and re-use.

1.05 Issuance and revocation of database access accounts shall be recorded in the PS 14.9 Log of Accounts Having Access to PHI.

2 PURPOSE

2.01 To secure personal health information from unauthorized access and maintain an accurate log of individuals having access to specific data holdings of PHI.

2.02 To disallow users of specific applications from accessing application related databases at the administrator level, thereby by-passing application-level controls such as user authentication, lockout, and maintenance of activity and data modification audit logs.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that database level access accounts/passwords are administered in the appropriate manner, monitored and audited.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.4 Issuing Database System Accounts and Passwords		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

4.02 It is the responsibility of the Privacy Officer to approve database level access accounts.

5 DEFINITIONS

5.01 A **Database System Account** is a low-level account that grants access to the underlying data tables and configuration of a database system.

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.1 Isolation of PHI Computers and Networks

PS 14.2 Issuing Network Accounts and Passwords

PS 14.3 Issuing Application Specific Accounts and Passwords

PS 14.5 Requirements for Access Accounts

PS 14.6 Requirements for Passwords

PS 14.7 Mandatory Password Expiry

PS 14.8 Limits on Password Re-Use

PS 14.9 Log of Accounts Having Access to PHI

PS 14.10 Decommissioning of Accounts upon Termination

PS 14.11 Maintaining Information Access Audit Logs

PS 14.12 Failed Authentication Account Lockout

7 PROCEDURE

7.01 Database system accounts are only assigned to Database and System Administrators of databases. The passwords of any database system accounts are only known to Database and System administrators.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.5 Requirements for Access Accounts		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Account/password combinations to access computer networks, applications, databases and other secured resources in respect of personal health information shall be required to restrict, control, and audit individuals access to these resources.

1.02 Any and all account names shall be unique to each individual and any account name shall be traceable to one and only one individual.

1.03 Account names shall be a minimum of 8 characters in length.

1.04 Account names shall be composed of a mix of alphabetic and numeric characters.

1.05 Account names shall not be re-used. If an account for an individual expires or is revoked that account name shall not be used in future, even if it would apply to the same individual.

1.06 Issuance, expiry and revocation of accounts shall be recorded in the PS 14.9 Log of Accounts Having Access to PHI.

1.07 Account names should not be comprised of:

(a) An individual's postal address
(b) An individual's date of birth
(c) A vehicle license plate number
(d) An individual's telephone number

1.08 Accounts should not be shared amongst two or more users.

2 PURPOSE

2.01 To secure personal health information from unauthorized access by enforcing best practices regarding naming of accounts, authenticating user access rights, and auditing access to data holdings of PHI by individuals.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that accounts names are issued and managed in accordance with this policy.

5 DEFINITIONS

5.01 An **Account Name** is the character string used to identify an individual user of a computer network, application, database system, or other secured resource.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.5 Requirements for Access Accounts		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.1 Isolation of PHI Computers and Networks

PS 14.2 Issuing Network Accounts and Passwords

PS 14.3 Issuing Application Specific Accounts and Passwords

PS 14.4 Issuing Database System Accounts and Passwords

PS 14.6 Requirements for Passwords

PS 14.7 Mandatory Password Expiry

PS 14.8 Limits on Password Re-Use

PS 14.9 Log of Accounts Having Access to PHI

PS 14.10 Decommissioning of Accounts upon Termination

PS 14.11 Maintaining Information Access Audit Logs

PS 14.12 Failed Authentication Account Lockout

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.6 Requirements for Passwords		Effective:	Sep 1, 2013
		Pages:	2
		Replaces:	Rev 1.0
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Each and every account to access a computer network, application, database, or other secured resource shall have a related password.

1.02 Each combination of account name and password shall be unique.

1.03 Passwords shall be a minimum of 10 characters in length.

1.04 Passwords shall be composed of a mix of alphabetic, numeric and non-alphanumeric characters, and contain both upper and lower case characters.

1.05 Except when originally issued, a password shall not be the same as the corresponding account name.

1.06 Passwords should not be comprised of:

(a) An individual's postal address
(b) An individual's date of birth
(c) A vehicle license plate number
(d) An individual's telephone number

1.07 Passwords should not be stored in human readable format within computer files, databases, on portable media, or paper records.

2 PURPOSE

2.01 To secure personal health information from unauthorized access by enforcing best practices regarding password composition and administration.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that passwords are issued and managed in accordance with this policy.

4.02 It is the responsibility of application developers to include appropriate password management functions that implement this policy in every application that accesses and manages data holdings of personal health information.

5 DEFINITIONS

5.01 A Password is an authentication string that in combination with a valid account name or User ID enables a person to access a computer network, application, database, or other secured resource.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.6 Requirements for Passwords		Effective:	Sep 1, 2013
		Pages:	2
		Replaces:	Rev 1.0
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.1 Isolation of PHI Computers and Networks

PS 14.2 Issuing Network Accounts and Passwords

PS 14.3 Issuing Application Specific Accounts and Passwords

PS 14.4 Issuing Database System Accounts and Passwords

PS 14.5 Requirements for Access Accounts

PS 14.7 Mandatory Password Expiry

PS 14.8 Limits on Password Re-Use

PS 14.9 Log of Accounts Having Access to PHI

PS 14.10 Decommissioning of Accounts upon Termination

PS 14.11 Maintaining Information Access Audit Logs

PS 14.12 Failed Authentication Account Lockout

7 PROCEDURE

7.01 When issuing a new password for an access account, do not communicate the account name and password combination in the same message to the intended user. Use separate messages and/or communication methods.

8 REVISION HISTORY

Revision 2.0 – August 30, 2013: Increases minimum password length to 10 characters (from 8) and adds the further requirement for including both upper and lower case characters in password composition in rule 1.04

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.7 Mandatory Password Expiry		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 When a new password is issued for an account by a system administrator the password shall expire immediately upon first use by the user, and the user shall be required to create a new password, known only to him/herself, in accordance with the composition rules specified in policy PS 14.6 Requirements for Passwords.

1.02 Active passwords on all accounts shall expire and require users to create a new password at least every 90 days from the date of the most recent password activation.

1.03 In the case of a security breach of a computer network, application, database or other secured resource, all accounts/passwords enabling access to the breached resource shall be expired and reset.

2 PURPOSE

2.01 To protect access accounts and passwords from unintended disclosure or "hacking" by limiting the time period during which an account/password combination is valid.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that passwords are set to expire in accordance with this policy and that users are notified about password expiry and provided the opportunity to create a new password.

4.02 It is the responsibility of application developers to include appropriate password management functions that implement this policy in every application that accesses and manages data holdings of personal health information.

4.03 It is the responsibility of each authorized user of a computer network, application, database or other secured resource containing personal health information to change his/her password upon expiry and when requested to do so by system administrators.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.1 Isolation of PHI Computers and Networks

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.7 Mandatory Password Expiry		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 14.2 Issuing Network Accounts and Passwords

PS 14.3 Issuing Application Specific Accounts and Passwords

PS 14.4 Issuing Database System Accounts and Passwords

PS 14.5 Requirements for Access Accounts

PS 14.6 Requirements for Passwords

PS 14.8 Limits on Password Re-Use

PS 14.9 Log of Accounts Having Access to PHI

PS 14.10 Decommissioning of Accounts upon Termination

PS 14.11 Maintaining Information Access Audit Logs

PS 14.12 Failed Authentication Account Lockout

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.8 Limits on Password Re-Use		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 When a user changes his/her password independently of a system administrator the user shall be prevented from changing the password to either of the last two (2) passwords used for that account.

2 PURPOSE

2.01 To protect access accounts and passwords from unintended disclosure or "hacking" by limiting the time period during which an account/password combination is valid.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of each authorized user of a computer network, application, database or other secured resource containing personal health information to change his/her password upon expiry and not re-use either of the last two (2) passwords.

4.02 It is the responsibility of application developers and system administrators to implement controls that prevent a user from re-using his/her last two passwords when changing a password.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.1 Isolation of PHI Computers and Networks

PS 14.2 Issuing Network Accounts and Passwords

PS 14.3 Issuing Application Specific Accounts and Passwords

PS 14.4 Issuing Database System Accounts and Passwords

PS 14.5 Requirements for Access Accounts

PS 14.6 Requirements for Passwords

PS 14.7 Mandatory Password Expiry

PS 14.9 Log of Accounts Having Access to PHI

PS 14.10 Decommissioning of Accounts upon Termination

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.8 Limits on Password Re-Use		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 14.11 Maintaining Information Access Audit Logs

PS 14.12 Failed Authentication Account Lockout

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.9 Log of Accounts Having Access to PHI		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A perpetual log of individuals access accounts to computer networks, applications, databases and other secured resources that contain personal health information shall be maintained as part of the PS 3.2 Privacy Document Archives.

1.02 The **Log of Accounts Having Access to PHI** shall contain the following minimum information:

(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

2 PURPOSE

2.01 To keep an up-to-date record of all persons who at one time or another were provided access to personal health information.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that the Log of Accounts Having Access to PHI is maintained accurate and up-to-date.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 5.2 Maintaining a Log of Authorized

PS 14.1 Isolation of PHI Computers and Networks

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.9 Log of Accounts Having Access to PHI		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 14.2 Issuing Network Accounts and Passwords

PS 14.3 Issuing Application Specific Accounts and Passwords

PS 14.4 Issuing Database System Accounts and Passwords

PS 14.5 Requirements for Access Accounts

PS 14.6 Requirements for Passwords

PS 14.7 Mandatory Password Expiry

PS 14.8 Limits on Password Re-Use

PS 14.10 Decommissioning of Accounts upon Termination

PS 14.11 Maintaining Information Access Audit Logs

PS 14.12 Failed Authentication Account Lockout

7 PROCEDURE

7.01 When a new account is created, or when an account is decommissioned, make an entry in the Log of Accounts Having Access to PHI located in the PS 3.2 Privacy Document Archives.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:			
PS 14.10 Decommissioning of Accounts upon Termination of Employment		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Upon termination of an individual's employment or contract with Inscyte Corporation or AIM Inc., each of the individual's access accounts to computer networks, applications, databases or other secured resources of personal health information shall be decommissioned.

1.02 If an employee or contractee of Inscyte Corporation or AIM Inc. ceases to require access to holdings of personal health information the individual's access accounts to computer networks, applications, databases or other secured resources of personal health information that are no longer required shall be decommissioned.

2 PURPOSE

2.01 To protect access accounts and passwords from unintended disclosure or "hacking" by disabling and deleting access accounts to holdings of personal health information that are no longer required.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that access accounts to holdings of personal health information are decommissioned upon termination of employment, contract or when the individual no longer requires access to holdings of PHI.

4.02 It is the responsibility of each employee or contractee of Inscyte Corporation or AIM Inc. to notify the Privacy Officer and Security Officer when he/she no longer requires access to personal health information.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.1 Isolation of PHI Computers and Networks

PS 14.2 Issuing Network Accounts and Passwords

PS 14.3 Issuing Application Specific Accounts and Passwords

PS 14.4 Issuing Database System Accounts and Passwords

PS 14.5 Requirements for Access Accounts

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:			
PS 14.10 Decommissioning of Accounts upon Termination of Employment		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 14.6 Requirements for Passwords

PS 14.7 Mandatory Password Expiry

PS 14.8 Limits on Password Re-Use

PS 14.9 Log of Accounts Having Access to PHI

PS 14.11 Maintaining Information Access Audit Logs

PS 14.12 Failed Authentication Account Lockout

7 PROCEDURE

7.01 To decommission an access account to a computer network, application, database or other secured resource, de-activate and delete the account from the affected system.

7.02 Record the decommissioning of the account in the Log of Individuals Having Access to PHI located in the PS 3.2 Privacy Document Archives.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.11 Maintaining Information Access Audit Logs		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Each time an individual uses or attempts to use his/her account/password to access a computer network, application, database or other secured resource containing personal health information, the action should be recorded in a perpetual Access Audit Log if a mechanism to do so can be implemented.

1.02 The **Access Audit Log** should contain the following minimum information:

(a) The account name
(b) The date/time of connection or attempt at connection
(c) Authentication status (successful or failed)
(d) Description of reason for authentication failure (if applicable)
(e) The name of the computer/device/URL from which the connection was made or attempted (if available)
(f) The date/time of connection termination (if available)

1.03 Access Audit Logs to computer networks, application, databases and other secured resources can reside with the secured resource to which the log applies.

1.04 Access Audit Logs shall not be deleted, only archived.

1.05 Access Audit Logs shall not be manually modified.

2 PURPOSE

2.01 To maintain a perpetual audit log of all authorized access to secured holdings of personal health information.

2.02 To provide a mechanism for monitoring attempts at access to secured holdings of personal health information that may be indicative of attempts at unauthorized access or “hacking”.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that Access Audit Logs are maintained where possible for each computer, network, application and/or database containing personal health information.

4.02 It is the responsibility of the Security Officer to ensure that access audit logs for secured holdings of personal health information are periodically reviewed to ascertain if activity indicative of an attempted breach of security has occurred.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.11 Maintaining Information Access Audit Logs		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

4.03 It is the responsibility of system administrators to inform the Security Officer and the Privacy Officer if activity indicative of an attempted breach of security is detected.

4.04 It is the responsibility of system developers and system administrators to implement the necessary controls on computer systems, networks, databases, and applications to maintain access audit logs and failed attempts at access.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.1 Isolation of PHI Computers and Networks

PS 14.2 Issuing Network Accounts and Passwords

PS 14.3 Issuing Application Specific Accounts and Passwords

PS 14.4 Issuing Database System Accounts and Passwords

PS 14.5 Requirements for Access Accounts

PS 14.6 Requirements for Passwords

PS 14.7 Mandatory Password Expiry

PS 14.8 Limits on Password Re-Use

PS 14.9 Log of Accounts Having Access to PHI

PS 14.10 Decommissioning of Accounts upon Termination

PS 14.12 Failed Authentication Account Lockout

PS 15.2 On-going Review of Security Logs

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.12 Failed Authentication Account Lockout		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 If each of three (3) consecutive attempts at using an account/password combination fail authentication, then:

(a) If the account name is valid, the account shall be immediately disabled or de-activated and,
(b) Where possible, an alert should be automatically communicated to the administrator(s) of the affected computer network, application, database or other secured resource.

2 PURPOSE

2.01 To detect and alert system administrators about possible attempts to breach security with respect to holdings of personal health information.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of system administrators to inform the Security Officer and the Privacy Officer if activity indicative of an attempted breach of security is detected.

4.02 It is the responsibility of system developers and system administrators to implement the necessary controls on computer systems, networks, databases, and applications to de-activate accounts following three failed authentications and send alerts to appropriate system administrators.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.1 Isolation of PHI Computers and Networks

PS 14.2 Issuing Network Accounts and Passwords

PS 14.3 Issuing Application Specific Accounts and Passwords

PS 14.4 Issuing Database System Accounts and Passwords

PS 14.5 Requirements for Access Accounts

PS 14.6 Requirements for Passwords

PS 14.7 Mandatory Password Expiry

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.12 Failed Authentication Account Lockout		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 14.8 Limits on Password Re-Use

PS 14.9 Log of Accounts Having Access to PHI

PS 14.10 Decommissioning of Accounts upon Termination

PS 14.11 Maintaining Information Access Audit Logs

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.13 CytoBase Data Modification Audit Logs		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 CytoBase shall incorporate a data modification audit log that lists all changes (inserts, updates, and deletes) to patient data elements and describes the date and time of the change, the name of the user account under which the change was performed, and the nature of the change.

2 PURPOSE

2.01 To provide an audit trail of all changes made to patient information from record inception through disposition.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the CytoBase database administrators and system developers to ensure that all changes to data, through inception to deletion are recorded in a read- only audit log.

4.02 It is the responsibility of CytoBase database administrators to archive the audit log(s) when appropriate.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.14 CytoBase Data Processing Audit Logs

PS 14.15 CytoBase Transmission Audit Logs

7 PROCEDURE

7.01 Refer to CytoBase (AIM ISIS-CSP) operating manual.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.14 CytoBase Data Processing Audit Logs		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 CytoBase shall incorporate a data processing audit log that lists all activities with respect to a patient record, such as initial record registration and all disclosure events describing the date and time of the activity, the name of the user account under which the activity was performed, and the nature of the activity.

2 PURPOSE

2.01 To provide an audit trail of handling and disclosure of patient information from record inception through disposition.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the CytoBase database administrators and system developers to ensure that all activities regarding patient data, through inception to deletion are recorded in a read- only audit log.

4.02 It is the responsibility of CytoBase database administrators to archive the audit log(s) when appropriate.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.13 CytoBase Data Modification Audit Logs

PS 14.15 CytoBase Transmission Audit Logs

7 PROCEDURE

7.01 Refer to CytoBase (AIM ISIS-CSP) operating manual.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.15 CytoBase Transmission Audit Logs		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 CytoBase shall incorporate data transmission audit logs that list all network transfers of patient records describing the date and time of the transfer, the sender and receiver, and a copy of the message transacted.

2 PURPOSE

2.01 To provide an audit trail of transmissions and enable messages to be re-processed in the event of a fault in the network transaction system.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the CytoBase system administrators and system developers to ensure that all network message transactions are logged and audited.

4.02 It is the responsibility of CytoBase database administrators to archive the transmission audit logs when appropriate.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.13 CytoBase Data Modification Audit Logs

PS 14.14 CytoBase Data Processing Audit Logs

7 PROCEDURE

7.01 Refer to CytoBase (AIM TRANSMED) operating manual.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.16 Backup and Recovery		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 All electronic holdings of personal health information, including specifically the CytoBase Oracle database, shall be copied to tape or other secondary storage media on a daily basis by taking a time-stamped snapshot of the data holdings.

1.02 The daily backup copies of the holdings of personal health information shall be retained in a secure location behind at least two physical security checkpoints.

1.03 Each daily backup copy shall be retained for a period of not less than seven days.

1.04 On the seventh day of the cycle, a weekly copy shall be created for off-site secure storage.

2 PURPOSE

2.01 To ensure that it is possible to restore continuity of operations and availability of data in the event of a failure in one or more components of the Datacenter.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that a daily backup copy of the CytoBase database and related data holdings of PHI is maintained in accordance with this policy.

5 DEFINITIONS

5.01 A **Physical Security Checkpoint** is a barrier to entry that requires a key, pass card or access code to open.

5.02 **The Datacenter** refers to the secured premises protected by two physical security checkpoints where the computing infrastructure (servers, storage arrays, network routers, back up devices etc.) is located.

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.17 Off-Site Storage of Backup Media

7 PROCEDURE

7.01 Refer to CytoBase operations manual and AIM disaster recovery plan.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.16 Backup and Recovery		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.17 Off-Site Storage of Backup Media		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A complete weekly backup copy of the CytoBase Oracle Database shall be stored in a secured off-site location.

1.02 The off-site backup copy shall be stored in a secured location behind at least two physical security checkpoints.

1.03 The off-site backup copy shall be protected against fire, water, or electro-magnetic damage.

2 PURPOSE

2.01 To ensure that it is possible to recover the CytoBase database in case of disastrous failure of the Datacenter.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that a weekly off-site backup copy of the CytoBase database is maintained in accordance with this policy.

5 DEFINITIONS

5.01 A **Physical Security Checkpoint** is a barrier to entry that requires a key, pass card or access code to open.

5.02 **The Datacenter** refers to the secured premises protected by two physical security checkpoints where the computing infrastructure (servers, storage arrays, network routers, back up devices etc.) is located.

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.16 Backup and Recovery

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.16 Backup and Recovery		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 17.6 Disaster Recovery Plan

7 PROCEDURE

7.01 Refer to CytoBase operations manual and disaster recovery plan.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.18 Acceptable Use of Remote Network Access		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 No remote network access shall be provided to the secure PHI network.

1.02 If remote network access is to be implemented for the business network the following precautions shall be implemented to protect the network:

(a) Remote access shall only be provided via a software/hardware virtual private network (VPN) solution.
(b) VPN access shall require authentication of an account/password combination
(c) Accounts/passwords shall be unique and traceable to an individual.
(d) Account names and passwords shall comply with the related provisions of these Privacy and Security Policies.

2 PURPOSE

2.01 To prevent remote access to holdings of personal health information.

2.02 To protect the business network against unauthorized access via a remote network connection.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that remote access to networks containing holdings of personal health information is prohibited.

4.02 It is the responsibility of the Security Officer to ensure that remote access to business networks is implemented in accordance with this policy and best practices regarding access security.

5 DEFINITIONS

5.01 **Remote Network Access** means gaining access to a local network via a connection over the public Internet.

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.1 Physical Isolation of Personal Health Information

PS 14.18 Acceptable Use of Remote Network Access

PS 14.20 Requirements for Internet Applications

7 PROCEDURE

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.18 Acceptable Use of Remote Network Access		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.19 Acceptable Use of Wireless Network Access		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 No wireless access shall be provided to the secure PHI network.

1.02 If local wireless access to the business network is to be implemented the following precautions shall be implemented to protect the network:

(a) The SSIDs of the wireless access points shall be changed from the default settings of the manufacturer access point device.
(b) Access shall be authenticated using strong WPA or WPA2 protocols only, not WEP.
(c) A log shall maintained of every device that is configured to connect to the wireless network.
(d) A mechanism shall be implemented to detect and remove rogue access points (i.e. someone purchasing a wireless access point device and connecting it to the business network.

2 PURPOSE

2.01 To prevent wireless access to holdings of personal health information.

2.02 To protect the business network against unauthorized access or eavesdropping via a wireless network.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that wireless access to networks containing holdings of personal health information is not implemented.

4.02 It is the responsibility of the Security Officer to ensure that wireless access to business networks is implemented in accordance with this policy and best practices regarding wireless access security.

5 DEFINITIONS

5.01 A **Wireless Access Point** is a device that connects to a TCP/IP wired network and listens to broadcast transmissions originating from equipment outfitted with IEEE 802.11 protocol transmitters.

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.1 Physical Isolation of Personal Health Information

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.19 Acceptable Use of Wireless Network Access		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 14.18 Acceptable Use of Remote Network Access

PS 14.20 Requirements for Internet Applications

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.20 Requirements for Internet Applications Accessing PHI		Effective:	Sep 1, 2013
		Pages:	3
		Replaces:	Rev 1
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Online applications shall be hosted on an Internet facing application server that is separate from the CytoBase database server(s).

1.02 Internet access to the application server shall be protected by a security firewall implemented between the Internet and the application server.

1.03 A second security firewall shall be implemented between the application server and the CytoBase database server(s) using internally specified ports and private security controls to connect the database. Standard RDBMS access ports are not to be used.

1.04 The application server shall be protected using a third party PKI certificate enabling encryption of data between the application server and a remote user's browser. Encryption strength should be 1024 bits or higher.

1.05 Internet applications shall implement unique accounts and passwords to authenticate each authorized user of the application.

1.06 With respect to **CytoBase**, only licensed Ontario healthcare providers in good standing shall be granted accounts to use the **CytoBase for Clinicians** online application.

1.07 To obtain a user account to access **CytoBase for Clinicians**, an individual shall register with Inscyte Corporation using a standard application form and provide the following information to verify his/her identity and authority to use the application:

(a) Full name
(b) Credentials and academic degrees
(c) OHIP Billing Number
(d) CPSO Registration Number (if applicable)
(e) Specialty
(f) Liability insurance provider and policy number
(g) Name of Institution (primary place of work)
(h) Full address
(i) Telephone
(j) Email address
(k) Photo ID

1.08 User accounts shall expire on an annual basis and require repeat registration.

1.09 User access to an internet application shall be monitored and audited.

1.10 Internet traffic relating to the application shall be monitored to detect any activity that may be indicative of a security attack.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.20 Requirements for Internet Applications Accessing PHI		Effective:	Sep 1, 2013
		Pages:	3
		Replaces:	Rev 1
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1.11 In the event a security attack is detected the application shall be de-activated until such time as the conditions and consequences relating to the attack are resolved.

1.12 Application server administrative consoles and administrative accounts shall be disabled for public facing applications such that an intruder cannot access any administrative files or services whatsoever.

1.13 Whenever possible, database connection parameters stored on web-application servers shall be strongly encrypted. This includes database domain names and/or IP addresses, IP ports, pooled login accounts and passwords.

1.14 Access to not required TCP services on web-application servers, such as TELNET (on port 23) , Secure Shell (SSH on port 22),and CHARGEN (on port 19) shall be disabled and/or blocked.

2 PURPOSE

2.01 To protect personal health information from unauthorized access, inadvertent disclosure, and tampering by enforcing strong security measures for online applications accessing CytoBase (i.e. CytoBase for Clinicians).

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that Internet applications that provide access to personal health information are hosted in accordance with this policy and implement best practices with respect to security controls and architecture to protect internet applications from attack.

4.02 It is the responsibility of the Privacy Officer to ensure that users of CytoBase for Clinicians are registered and verified using the prescribed application process.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

None

7 PROCEDURE

7.01 Standard application forms and instructions for registering users of CytoBase for Clinicians can be obtained from the PS 3.2 Privacy Document Archives.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.20 Requirements for Internet Applications Accessing PHI		Effective:	Sep 1, 2013
		Pages:	3
		Replaces:	Rev 1
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

8 REVISION HISTORY

Revision 2.0 – August 30, 2013: Rule 1.03 adds the stipulation that "Standard RDBMS access ports are not to be used". New rules 1.12, 1.13, and 1.14 added.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.21 Policy and Procedure for Patch Management		Effective:	Oct 31, 2014
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Approved
Issued by:	Privacy Officer	Dated:	Oct 10, 2014

1 POLICY

1.01 Inscyte Corporation's computing infrastructure for CytoBase shall be configured and continuously upgraded in accordance with these policies to ensure that the computing infrastructure is secure against known vulnerabilities in operating systems, network and computing devices, and application software.

1.02 Complete and accurate asset inventory documentation shall be maintained for all components of the CytoBase computing infrastructure, including operating systems, computing and network devices, and application software, to ensure that all components are accounted for when researching and applying patches.

1.03 Availability of patches for system components shall be researched and reviewed on a monthly basis, and where possible, automated methods of notification from vendors shall be implemented.

1.04 Patches shall be categorized as critical, routine or low priority. Determination of priority shall be based on vendor/market reported severity (high, medium, low) and the existence of know exploits that use the vulnerability being patched as follows:

Critical Priority:	High severity vulnerabilities Medium severity vulnerabilities with known exploits
Routine Priority:	Medium severity vulnerabilities with no known exploits
Low Priority:	Low severity vulnerabilities

1.05 Patches shall be applied in accordance with the following schedule:

Critical Priority:	At the earliest available opportunity
Routine Priority:	No later than three (3) months of availability
Low Priority:	No later than six (6) months of availability

1.06 All vendor-recommended patches shall be applied in accordance with the above prioritization and scheduling policies, subject to the provisions of policies 1.07 through 1.10

1.07 Patches can be applied without the express authorization of Inscyte Corporation unless there is reason to believe that a patch will significantly degrade system performance, the strength of security controls, functionality, or require additional funding. In these cases, the patch is to be brought to the attention of the Security Officer and the Board of Inscyte for review and recommendations.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.21 Policy and Procedure for Patch Management		Effective:	Oct 31, 2014
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Approved
Issued by:	Privacy Officer	Dated:	Oct 10, 2014

1.08 In the event that a determination is made that a patch should not be implemented, the determination shall be documented in the CytoBase System Configuration Change Log, including:

- A description of the patch
- The date of availability
- The severity/priority of the patch
- The affected software/hardware components
- The rationale/reason for not implementing the patch
- The agent/personnel making the entry

1.09 Patches published by trusted vendors (e.g. Microsoft, Oracle) do not require testing provided that there is a rollback mechanism to revert to a known good state. Patches to user application software require testing and QA prior to release in a production setting.

1.10 All applied patches are to be recorded in the CytoBase System Configuration Change Log, with the following information:

- A description of the patch
- The date of availability
- The severity/priority of the patch
- The affected software/hardware components
- The date the patch was tested (if applicable)
- The agents/personnel that tested the patch (if applicable)
- The date the patch was implemented in production
- The agents/personnel that implemented the patch

2 PURPOSE

2.01 The objective of Inscyte Corporation's patch management program is to create and maintain a consistently configured and documented computing environment that is secure against known vulnerabilities in operating systems, network and computing devices, and application software.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 The Security Officer has overall responsibility for implementing the patch management program and ensuring on-going compliance with these policies and procedures.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.21 Policy and Procedure for Patch Management		Effective:	Oct 31, 2014
		Pages:	3
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Approved
Issued by:	Privacy Officer	Dated:	Oct 10, 2014

4.02 The Security Officer may delegate the day-to-day work in respect of patch management to Inscyte Corporation's Agent, AIM Inc., which shall be responsible for:

a) Monitoring and researching the availability of patches.
b) Alerting administrators and users about security issues.
c) Prioritizing and applying patches in accordance with these policies.
d) Performing patch testing and QA in accordance with these policies.
e) Maintaining a complete and accurate asset inventory to ensure that all components of the CytoBase computing infrastructure are accounted for when researching and applying patches.
f) Maintaining the CytoBase System Configuration Change Log.

5 DEFINITIONS

5.01 A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance.

5.02 Patch management is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.

6 REFERENCES and related POLICIES & PROCEDURES

PS 17.2 Asset Inventory and Configuration Information

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.22 Remote Network Access		Effective:	Nov 16, 2016
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Approved
Issued by:	Security Officer	Dated:	Nov 16, 2016

1 POLICY

1.01 Remote network access shall be granted to individuals for a specified period of time. Authorization for remote access is made by the individual's supervisor and the security officer and must be based on justifiable need rather than convenience.

1.02 Remote network access shall be provided only to the business network and / or user Desktop only.

1.03 The maximum authorized duration of remote access rights shall be three (3) months, whereupon any extension must be authorized again in accordance with this policy.

1.04 Remote access shall only be provided via a secured software/hardware virtual private network (VPN) solution.

(a) VPN access shall require authentication of an account/password combination along with a secondary authentication.
(b) Accounts/passwords shall be unique and traceable to an individual.
(c) Account names and passwords shall comply with the related provisions of these Privacy and Security Policies.

2 PURPOSE

2.01 To allow remote access by AIM employees to business network.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to allow remote access to the business network.

4.02 It is the responsibility of the Security Officer to ensure that remote access to business networks is maintained in accordance with this policy and best practices regarding access security.

5 DEFINITIONS

5.01 **Remote Network Access** means gaining access to the local business network via a secure and encrypted connection over the public Internet.

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.18 Acceptable Use of Remote Network Access

PS 14.20 Requirements for Internet Applications

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	14 Information Security		
PS 14.22 Remote Network Access		Effective:	Nov 16, 2016
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Approved
Issued by:	Security Officer	Dated:	Nov 16, 2016

7 PROCEDURE

7.01 Request for remote access is made by filling in the standard VPN request form which must be signed by the applicant and his/her supervisor. It is then forwarded to the security officer for signed authorization.

7.02 Remote access is provided only during the access dates stated in the request form.

7.03 Signed and approved request forms are scanned and saved in the Log of Remote Network Access

7.04 All requests for remote network access are recorded in the log of Remote Network Access.

8 REVISION HISTORY

None

15 Security Audit Program

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	15 Security Audit Program		
PS 15.1 Conducting Security Audits		Effective:	May 26, 2017
		Pages:	3
		Replaces:	Rev 3
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A security audit shall be conducted on an quarterly basis to assess security risks and whether current security controls are adequate to mitigate the identified risks.

1.02 The security audit program should adhere to ISO/IEC 27002 Information Security Standards, covering the following:

1) Risk assessment
2) Security policy - management direction
3) Organization of information security - governance of information security
4) Asset management - inventory and classification of information assets
5) Human resources security – access rights of employees joining, moving and leaving the organization
6) Physical and environmental security - protection of the computer facilities and premises where personal health information is stored
7) Communications and operations management - management of technical security controls in systems and networks
8) Access control - restriction of access rights to networks, systems, applications, functions and data
9) Information systems acquisition, development and maintenance - building security into applications
10) Information security incident management - anticipating and responding appropriately to information security breaches
11) Business continuity management - protecting, maintaining and recovering business-critical processes and systems
12) Compliance - ensuring conformance with information security policies, standards, laws and regulations

1.03 A **Security Audit Report** shall be prepared for management review following each security audit. The Security Audit Report shall describe each audit activity undertaken, when the activity was performed, by whom, the results of the audit (findings), and recommendations to correct any deficiencies identified.

2 PURPOSE

2.01 To ensure that the 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.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	15 Security Audit Program		
PS 15.1 Conducting Security Audits		Effective:	May 26, 2017
		Pages:	3
		Replaces:	Rev 3
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

2.02 To ensure that the information security program complies with all applicable legislation and keeps pace with emerging best practices.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that a security audit is conducted on an annual basis.

4.02 It is the responsibility of the Security Officer to conduct the security audits.

4.02 It is the responsibility of the Privacy Officer to review and sign-off on **Security Audit Reports** and to ensure that appropriate changes are made to the **Consolidated Log of Recommendations**.

5 DEFINITIONS

5.01 A **Security Audit** is a self-assessment tool and methodology to ensure that security policies, procedures, and controls are managed using best practices to ensure the on-going confidentiality, integrity and availability of sensitive information.

6 REFERENCES and related POLICIES & PROCEDURES

PS 12.7 Log of Individuals Having Access to Premises

PS 14.9 Log of Accounts Having Access to PHI

PS 15.3 Maintaining a Log of Security Audits

PS 16.4 Log of Security Breaches

PS 17.2 Asset Inventory and Configuration Information

PS 17.4 Conducting Threat Risk Assessments

PS 17.3 Consolidated Log of Recommendations

PS 17.5 Corporate Risk Register

PS 17.6 Disaster Recovery Plan

PS 10.3 Conducting Privacy Audits

7 PROCEDURE

7.01 Conduct as security audit by reviewing the following information:

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	15 Security Audit Program		
PS 15.1 Conducting Security Audits		Effective:	May 26, 2017
		Pages:	3
		Replaces:	Rev 3
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1) **Log of Security Breaches** – analyze nature/cause of breaches and recommend solutions to prevent recurrence.
2) **Asset Inventory and Configuration Information** – review to ascertain accuracy and completeness. Assess adequacy of security controls and recommend upgrades as appropriate.
3) **Threat Risk Assessment** – review the latest TRAs to ascertain accuracy and completeness and update as required to align with current assets and processes. Assess adequacy of current security controls and recommend upgrades as appropriate.
4) **Disaster Recovery Plan** – review the latest DRP to ascertain accuracy and completeness. Update as required.
5) **Log of Individuals Accounts Having Access to PHI** – review to ascertain accuracy and completeness and if individuals continue to require access rights (update as necessary and terminate access rights as necessary). Assess adequacy of computer security controls and recommend upgrades as appropriate.
6) **Log of Individuals Having Access to Premises** – review to ascertain accuracy and completeness and if individuals continue to require access rights (update as necessary and terminate access rights as necessary). Assess adequacy of physical security controls and recommend upgrades as appropriate.

7.02 Prepare a **Security Audit Report** from the findings above listing the audit activity performed, the date, who performed the activity, findings and recommendations.

7.03 Provide the report to the Privacy Officer for review and sign-off.

7.04 Update the **Consolidated Log of Recommendations** as appropriate.

7.05 Store the Security Audit Report in the **Log of Security Audits** section of the Privacy Document Archives.

7.06 Update the **Log of Security Audits** to record the audit activity.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	15 Security Audit Program		
PS 15.2 On-going Review of Security Logs		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Security Logs shall be reviewed on a regular basis to monitor access to secured premises and personal health information to detect activity that may be indicative of a security breach or attempted breach.

1.02 Security Logs should be monitored on a monthly basis at minimum, preferable on a weekly basis.

1.03 Activity that may be indicative of a security breach or attempted breach shall be reported immediately to the Security Officer and the Privacy Officer for direction on resolution.

2 PURPOSE

2.01 To proactively monitor access to secured premises and access/use of personal health information to detect and/or prevent security breaches.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that security logs are monitored and inspected on a regular basis.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 14.11 Maintaining Information Access Audit Logs

PS 16.1 Identifying a Breach

PS 16.2 Reporting a Breach

PS 16.3 Actions Following a Breach

PS 16.4 Log of Security Breaches

7 PROCEDURE

7.01 Monitor and inspect the following: Datacenter access logs, CytoBase transmission logs, CytoBase for Clinicians web statistics.

8 REVISION HISTORY

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	15 Security Audit Program		
PS 15.2 On-going Review of Security Logs		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	
None			

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	15 Security Audit Program		
PS 15.3 Maintaining a Log of Security Audits		Effective:	Nov 1, 2011
		Pages:	1
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A perpetual **Log of Security Audits** shall be maintained in the Privacy Document Archives.

1.02 The **Log of Security Audits** shall contain the following minimum information:

(a) The date the audit was initiated
(b) The name of the person who initiated the audit
(c) The name of the file containing the Security Audit Report for that audit

2 PURPOSE

2.01 To maintain an accurate and complete record of all Security Audits performed.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that the Log of Security Audits is kept up-to-date and accurate.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 15.1 Conducting Security Audits

PS 3.2 Privacy Document Archives

7 PROCEDURE

7.01 The Log of Security Audits is a Microsoft Excel file located in the Privacy Document Archives – Section: Log of Security Audits.

7.02 Make an entry in this file for each security audit performed.

8 REVISION HISTORY

None

16 Security Breach Management

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	16 Security Breach		
PS 16.1 Identifying a Breach of Security		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A breach of security occurs whenever a person has gained, or attempts to gain, unauthorized access to secured premises or secured information.

1.02 A breach of security may be reported via a complaint or challenge to compliance with these policies and procedures filed by a third party.

1.03 A breach of security may be self-identified through the course of everyday work.

1.04 Subject to the definition below, a breach of security or a potential breach may be signaled by the discovery that:

(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

1.05 The first course of action upon discovering a breach of security is to contain the breach in accordance with policy: PS 16.3 Actions Following a Breach of Security.

1.06 Any individual who identifies a breach of security shall report the incident to the Security Officer as soon as possible and in accordance with policy: PS 16.2 Reporting a Breach of Security.

2 PURPOSE

2.01 To provide a definition of a breach of security and describe the circumstances that may signal that a breach of security has occurred or may occur.

2.02 To foster an environment where every individual is vigilant and proactive with respect to safeguarding personal health information.

2.03 Section 12(1) of the Act requires Inscyte Corporation, and by extension AIM Inc. as agent of Inscyte, to take steps that are reasonable in the circumstances to ensure personal health information is protected against theft, loss and unauthorized use or disclosure, and to ensure that records containing personal health information are protected against unauthorized access, copying, modification or disposal.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	16 Security Breach		
PS 16.1 Identifying a Breach of Security		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of each member of the staff of Inscyte Corporation and its agents to be vigilant of and identify breaches (or potential breaches) of security and report these as soon as possible so that a breach of security can be contained and managed, and that mitigating actions can be taken to prevent similar breaches from occurring in the future.

5 DEFINITIONS

5.01 A **Breach of Security** is defined 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.

5.02 A breach of security occurs in the above circumstances regardless of the consequences of the breach, which could include a breach of privacy.

6 REFERENCES and related POLICIES & PROCEDURES

PS 16.2 Reporting a Breach of Security

PS 16.3 Actions Following a Breach of Security

PS 16.4 Log of Security Breaches

PS 11.1 Indentifying a Breach of Privacy

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	16 Security Breach		
PS 16.2 Reporting a Breach of Security		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Any individual who discovers a breach or potential breach of security shall immediately notify the Privacy Officer and Security Officer of the incident either verbally or by email.

1.02 A Security Breach Report shall be prepared for each incident of breach.

1.03 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 then a Breach of Privacy shall be reported in accordance with policies PS 11.2 Reporting a Breach of Privacy and PS 11.3 Actions Following a Breach of Privacy.

2 PURPOSE

2.01 To ensure breaches of security are reported to the appropriate parties and in accordance with legislative requirements, including, but not limited to Ontario's *Personal Health Information Protection Act, 2004* (the Act).

2.02 To document breaches of security with sufficient information so that mitigating actions can be taken to prevent similar breaches from occurring in the future.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of each member of the staff of Inscyte Corporation and its agents to identify breaches (or potential breaches) of security and report these as soon as possible so that actions can be taken to contain the breach and mitigating actions taken to prevent similar breaches from occurring in the future.

4.02 It is the responsibility of the Security Officer to notify the Privacy Officer of reported security breaches and ensure that all breaches are fully documented.

5 DEFINITIONS

5.01 See definition of a **Breach of Security** in policy: PS 16.1 Identifying a Breach of Security.

6 REFERENCES and related POLICIES & PROCEDURES

PS 16.1 Identifying a Breach of Security

PS 16.3 Actions Following a Breach of Security

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	16 Security Breach		
PS 16.2 Reporting a Breach of Security		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 16.4 Log of Security Breaches

PS 11.2 Reporting a Breach of Privacy

7 PROCEDURE

7.01 To prepare a **Security Breach Report**, access AIM's PS 3.2 Privacy Document Archives, Section: Log of Security Breaches and open a Breach Report template. Fill out the report as completely as possible. Send the report to the Privacy Officer for review and approval.

7.02 In all cases of breach initiate policy and procedure 0 PS 16.3 Actions Following a Breach of Security.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	16 Security Breach		
PS 16.3 Actions Following a Breach of Security		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Upon discovery of a breach of security (or suspected breach of security) assess the incident to determine if a breach of privacy has also occurred. If so, the provisions and procedures of policy: PS 11.3 Actions Following a Breach of Privacy take precedence.

1.02 Upon discovery of a security breach the following actions shall be taken:

1. Assess the incident
2. Contain the breach
3. Notify Security Officer and Privacy Officer
4. Prepare a report of the breach
5. Investigate and remediate the breach
6. Complete the security breach report
7. Approve report and recommendations for mitigating strategies

Depending on the severity of the breach, these actions may have to be undertaken simultaneously, or in very short succession. Refer to the procedures below for details on these steps.

2 PURPOSE

2.01 To respond quickly, effectively and in a coordinated manner in case of a breach of security.

2.02 To contain the breach and thereby limit the severity of the consequences.

2.03 To document the breach and make remediation efforts easier.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of each and every employee to implement the actions following a breach of security (i.e. the breach protocol) immediately upon discovering a breach of security or suspected breach of security.

5 DEFINITIONS

5.01 See definition of a **Breach of Security** in policy: PS 16.1 Identifying a Breach.

6 REFERENCES and related POLICIES & PROCEDURES

PS 11.1 Indentifying a Breach of Privacy

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	16 Security Breach		
PS 16.3 Actions Following a Breach of Security		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 16.2 Reporting a Breach of Security

PS 16.4 Log of Security Breaches

PS 11.3 Actions Following a Breach of Privacy

7 PROCEDURE

7.01 **Assess the Incident** – Assess the incident to determine if a breach of privacy has also occurred or is likely to occur as a result of the security breach. If so, proceed in accordance with policy: PS 11.3 Actions Following a Breach of Privacy.

Assess the extent of the security breach to determine which security controls have or may have been compromised and by what means. Decide if these controls are to be "locked down" to prevent further security breaches.

7.02 **Contain the Breach** – Take all necessary actions to secure the premises or information holdings affected by the breach even if this means suspending access to authorized individuals. This may require recovering access keys, pass cards, re-setting access codes and, accounts, or even taking computer systems off-line etc.

7.03 **Notify Appropriate Personnel** – Notify the Security Officer & Privacy Offcier

7.04 **Prepare a Report of the Breach** – Acquire the template Security Breach Report from AIM's PS 3.2 Privacy Document Archives, Section: Log of Security Breaches, and prepare a report of the breach. Send the report to AIM's Privacy Officer for review.

7.05 **Investigate and Remediate** – Investigate the circumstances and motivation behind the breach. The Security Breach Report should contain information on the cause and/or reason for the breach, and recommendations for remediation measures to mitigate or prevent similar breaches from occurring in the future.

7.06 **Complete the Breach Report** – Send the final Breach Report to the Security Officer for sign-off. Upon sign-off the Security Officer may distribute the report to all stakeholders involved.

7.07 **Approve report and recommendations for mitigating strategies** – The Security Officer is required to ensure that all recommendations are brought forward and recorded in the PS 17.3 Consolidated Log of Recommendations.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	16 Security Breach		
PS 16.4 Log of Security Breaches		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 A perpetual Log of Security Breaches shall be maintained that describes each incident of breach in the form of a **Security Breach Report**.

1.02 A **Security Breach Report** shall contain the following minimum information:

(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

1.03 To finalize a **Security Breach Report**, the report shall be reviewed and signed-off by the Privacy Officer.

2 PURPOSE

2.01 To document each incident of a breach of privacy for future reference.

2.02 To provide a record of remedial actions and mitigation strategies to prevent similar occurrences in the future.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that the Log of Security Breaches is complete and up-to-date.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	16 Security Breach		
PS 16.4 Log of Security Breaches		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

5 DEFINITIONS

5.01 See definition of a **Breach of Security** in policy: 0 PS 16.1 Identifying a Breach of Security.

6 REFERENCES and related POLICIES & PROCEDURES

PS 16.1 Identifying a Breach of Security

PS 16.2 Reporting a Breach of Security

PS 16.3 Actions Following a Breach of Security

PS 11.4 Log of Privacy Breaches

7 PROCEDURE

7.01 To prepare a **Security Breach Report** acquire the template breach report from AIM's privacy and security document archives and fill out the report. Send the report to the Privacy Officer for review and approval.

7.02 Use the following **file naming** convention to distinguish each breach report:

SBR-<*incident name*>-<*incident date*>.doc

Where:

SBR-	The standard prefix for Security Breach Report
<*incident name*>	A short name for the incident
<*incident date*>	The date of discovery in the form yyyy-mmm-dd
Example:	BR-Misplaced CytoBase Tape-2011-May-14.doc

7.03 When a breach report is completed, convert the document to a **read-only file** format (such as Adobe PDF) with the same file name.

8 REVISION HISTORY

None

17 Risk Management and Business Continuity

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	17 Risk Management and Business Continuity		
PS 17.1 Risk Management Framework		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte Corporation and AIM Inc. shall have in place a framework of policies and procedures to identify and manage risk with respect to the safeguarding personal health information and its availability.

1.02 Identified risks shall be communicated to the Privacy Officer and Security Officer, and recorded in the **Corporate Risk Register**.

1.03 Each identified risk shall be promptly assessed and recommendations made to mitigate the risk. These recommendations shall be recorded in the **Consolidated Log of Recommendations**.

1.04 The **Corporate Risk Register** and **Consolidated Log of Recommendations** shall be reviewed at least quarterly to ensure appropriate measures are being taken to monitor and mitigate risks.

2 PURPOSE

2.01 To ensure that risks are identified, recorded, assessed (ranked), and acted upon so as to monitor the risks and mitigate the potential negative consequences of the risks.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the President of Inscyte and the CEO of AIM Inc. to ensure that a Risk Management Framework is implemented to identify, document, and mitigate risks.

4.02 It is the responsibility of the Security Officer to ensure that identified risks are recorded in the PS 17.5 Corporate Risk Register, that each risk is assessed (ranked) and that recommendations are brought forward to mitigate the identified risks.

4.03 It is the responsibility of the Security Officer to ensure that recommendations are recorded in the PS 17.3 Consolidated Log of Recommendations.

4.03 It is the responsibility of each employee or contractee of Inscyte Corporation and AIM Inc. to identify and report risks to either the Security Officer or the Privacy Officer.

5 DEFINITIONS

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	17 Risk Management and Business Continuity		
PS 17.1 Risk Management Framework		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

5.01 A **Risk** is the probability of one or more future events occurring , the consequences of which would lead to a breach of privacy, security, and/or the availability of information or information management resources.

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.2 Privacy Document Archives

PS 17.2 Asset Inventory and Configuration Information

PS 17.3 Consolidated Log of Recommendations

PS 17.4 Conducting Threat Risk Assessments

PS 17.5 Corporate Risk Register

PS 17.6 Disaster Recovery Plan

7 PROCEDURE

7.01 If a risk is identified, report the risk via email message or other document to the Security Officer and/or the Privacy Officer.

7.02 Record the risk in the Corporate Risk Register, found in the Privacy Document Archives.

7.03 Assess the risk to determine its probability of occurrence and severity/impact of the consequences should the risk materialize.

7.04 Record recommendations for monitoring and mitigating the risk in the Corporate Risk Register and also in the Consolidated Log of Recommendations, both found in the Privacy Document Archives.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	17 Risk Management and Business Continuity		
PS 17.2 Asset Inventory and Configuration Information		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte Corporation and AIM Inc. shall maintain an inventory of all assets pertaining to the CytoBase computing infrastructure together with configuration information for each asset.

1.02 The **Asset Inventory** shall be updated each time that an asset is modified, upgraded, decommissioned or when a new asset is added to inventory.

1.03 Whenever a change to the computing and security infrastructure is contemplated a risk assessment shall be conducted to determine if the change negatively affects the existing privacy and/or security measures. The findings shall be documented in the Asset Inventory.

1.04 If the risk assessment reveals a negative impact, the risk shall be reported to the Privacy Officer for review and determination of whether or not a Privacy Impact Assessment is required. This determination shall be documented in the Asset Inventory.

2 PURPOSE

2.01 To document the components of the computing and security infrastructure so that these can be easily replaced/repaired and properly configured when the need to do so arises.

2.02 To maintain a record of changes to the computing and security infrastructure together with risk assessments and determinations of whether or not a Privacy Impact Assessment was warranted or not.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that the Asset Inventory and configuration information is maintained accurate, complete and up-to-date.

4.02 It is the responsibility of the Security Officer to ensure that a risk assessment is conducted with respect to all changes to the computing infrastructure, and that the finding are documented in the Asset Inventory.

4.03 It is the responsibility of the Privacy Officer to review risk assessments when changes to the computing infrastructure are contemplated and make a determination of whether or not the change(s) warrant a Privacy Impact Assessment, and to document the determination in the Asset Inventory.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	17 Risk Management and Business Continuity		
PS 17.2 Asset Inventory and Configuration Information		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

5 DEFINITIONS

5.01 An **Asset** is a component of the computing and security infrastructure, including supporting software and hardware, such as operating systems, database systems, application software, servers, routers, security checkpoints, alarm systems and so on.

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.2 Privacy Document Archives

PS 10.1 Conducting Privacy Impact Assessments

PS 17.1 Risk Management Framework

PS 17.3 Consolidated Log of Recommendations

PS 17.4 Conducting Threat Risk Assessments

PS 17.5 Corporate Risk Register

PS 17.6 Disaster Recovery Plan

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	17 Risk Management and Business Continuity		
PS 17.3 Consolidated Log of Recommendations		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte Corporation and AIM Inc. shall maintain a **Consolidated Log of Recommendations** arising from privacy impact assessments, privacy audits, security audits, threat/risk assessments, the investigation of privacy/security breaches, and reviews by the Information and Privacy Commissioner of Ontario.

1.02 The **Consolidated Log of Recommendations** shall contain the following minimum information:

(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

1.03 The **Consolidated Log of Recommendations** shall be updated as appropriate 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

1.04 The **Consolidated Log of Recommendations** shall be retained in perpetuity in the privacy document archives.

2 PURPOSE

2.01 To maintain a centralized record and bookkeeping system that tracks all recommendations made with respect to the privacy/security program and record how each recommendation was addressed.

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	17 Risk Management and Business Continuity		
PS 17.3 Consolidated Log of Recommendations		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that the Consolidated Log of Recommendations is maintained accurate, complete, an and up-to-date.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.2 Privacy Document Archives

PS 17.1 Risk Management Framework

PS 17.2 Asset Inventory and Configuration Information

PS 17.4 Conducting Threat Risk Assessments

PS 17.5 Corporate Risk Register

PS 17.6 Disaster Recovery Plan

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	17 Risk Management and Business Continuity		
PS 17.4 Conducting Threat Risk Assessments		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Formalized **Threat/Risk Assessments** (TRA) shall be conducted on all holdings of personal health information and assets of the related computing infrastructure whenever there is a change to the asset inventory or to the nature of the data holdings.

1.02 The TRA shall include:

(a) Identification of the asset under consideration
(b) Ranking of the asset sensitivity
(c) Identification of the agent(s) of threat for the asset
(d) Ranking of the agent(s) threat in terms of capability and motivation
(e) Identification of the agent-events that would place the asset at risk
(f) Ranking each risk with respect to the likelihood of occurrence and impact
(g) Recommendations to mitigate highly ranked risks
(h) The date and name of the person who performed the TRA

1.03 All TRAs shall be retained in perpetuity in the Privacy Document Archives

2 PURPOSE

2.01 To implement a systematized process of measuring risks on an on-going basis as changes occur in the holdings of personal health information or the computing infrastructure.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to conduct and document a TRA each time there is a change to the computing infrastructure or there is a change in the nature of the holdings of personal health information.

5 DEFINITIONS

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.2 Privacy Document Archives

PS 17.1 Risk Management Framework

PS 17.2 Asset Inventory and Configuration Information

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	17 Risk Management and Business Continuity		
PS 17.4 Conducting Threat Risk Assessments		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

PS 17.3 Consolidated Log of Recommendations

PS 17.5 Corporate Risk Register

PS 17.6 Disaster Recovery Plan

7 PROCEDURE

7.01 See "TRA Guidelines" in the Privacy Document Archives – Section: Threat Risk Assessments.

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	17 Risk Management and Business Continuity		
PS 17.5 Corporate Risk Register		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte Corporation and AIM Inc. shall maintain a **Corporate Risk Register** listing risks identified outside of a formal Threat/Risk assessment that may negatively affect the ability to safeguard the confidentiality of personal health information, its accuracy, and availability.

1.02 The **Corporate Risk Register** shall contain the following minimum amount of information:

(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

1.03 The **Corporate Risk Register** shall be updated whenever a new risk is identified which usually coincides with changes to operating procedures or technology.

1.04 The **Corporate Risk Register** shall be maintained in perpetuity in the Privacy Document Archives

2 PURPOSE

2.01 To implement a systematized process of recording identified risks and the strategies taken to mitigate these risks.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Privacy Officer to ensure that the Corporate Risk Register is maintained accurate, complete, an and up-to-date.

5 DEFINITIONS

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	17 Risk Management and Business Continuity		
PS 17.5 Corporate Risk Register		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 3.2 Privacy Document Archives

PS 17.1 Risk Management Framework

PS 17.2 Asset Inventory and Configuration Information

PS 17.3 Consolidated Log of Recommendations

PS 17.4 Conducting Threat Risk Assessments

PS 17.6 Disaster Recovery Plan

7 PROCEDURE

7.01 None

8 REVISION HISTORY

None

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	17 Risk Management and Business Continuity		
PS 17.6 Disaster Recovery Plan		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

1 POLICY

1.01 Inscyte Corporation and AIM Inc. shall maintain a comprehensive **Disaster Recovery Plan** and associated documentation to recover from a catastrophic disruption of services and/or loss of availability of personal health information.

1.02 The **Disaster Recovery Plan** shall address:

(a) Procedure for notification of stakeholders
(b) Procedure to assess the cause and impact of the disruption
(c) Procedure to assess the damage from the disruption
(d) Procedure to assess and address the potential of a breach of privacy occurring as a consequence of the disruption.
(e) Where to find contact lists (stakeholders/vendors etc.)
(f) Where to find asset Inventory and Configuration Information
(g) Where to find backup media
(h) Where to find software media
(i) Procedures for recovery and restoration of lost assets and data holdings
(j) The agent(s)/person(s) responsible for carrying out all parts of the plan

1.03 The **Disaster Recovery Plan** and all related documentation shall be maintained in perpetuity in the Privacy Document Archives and one copy shall be stored on portable media, maintained off-site.

1.04 The **Disaster Recovery Plan** shall be updated whenever a change in the computing infrastructure occurs.

2 PURPOSE

2.01 A process and documentation is required to ensure that business continuity can be restored in the event of natural, human, environmental, and/or technical disruptions to the computing infrastructure in the short and long term, and to safeguard personal health information during the recovery process.

3 SCOPE

3.01 This policy applies to Inscyte Corporation and to AIM Inc. as its agent.

4 RESPONSIBILITY

4.01 It is the responsibility of the Security Officer to ensure that a comprehensive Disaster Recovery Plan and all required information are maintained accurate, complete and up-to-date.

5 DEFINITIONS

Statement of Policy & Procedure			
Chapter:	Privacy & Security		
Section:	17 Risk Management and Business Continuity		
PS 17.6 Disaster Recovery Plan		Effective:	Nov 1, 2011
		Pages:	2
		Replaces:	New
Issued to:	All Manual Holders	Approval:	Final
Issued by:	Privacy Officer	Dated:	

5.01 None

6 REFERENCES and related POLICIES & PROCEDURES

PS 17.1 Risk Management Framework

PS 17.2 Asset Inventory and Configuration Information

PS 17.3 Consolidated Log of Recommendations

PS 17.4 Conducting Threat Risk Assessments

PS 17.5 Corporate Risk Register

7 PROCEDURE

None

8 REVISION HISTORY

None