Privacy Policy

Version 1.12

November 28, 2012

144 Front Street West, Suite 300, Toronto, Ontario M5J 2L7 • T 416.483.5974 F 416.483.9197 • www.healthtech.ca

Table of Contents

1. Document Control

Date	Author	Changes	Version
August 26, 2008	Karen Keith	Initial version for approval by Senior Management	V1.0
November 12, 2008	Karen Keith	Minor language changes	V1.1
December 4, 2008	Karen Keith	Minor language changes after review by Senior Management	V1.2
December 10, 2008	Karen Keith	Modification of Confidentiality Agreement	V1.3
January 27, 2009	Karen Keith	Modification based on associate review and consultation	V1.4
May 15, 2009	Karen Keith	Slight modification	V1.5
November 24, 2009	Karen Keith	Modification based on HT input	V1.6
March 22, 2011	Karen Waite	Proposed revisions/comments	V1.7
March 24, 2011	Karen Waite	Further revisions based on conversation with Karen Keith	V 1.8
April 4, 2011	Karen Waite	Further revisions based on Karen Keith review	V 1.9
June 29, 2011	Karen Waite	Further revisions based on review by Mary Jane Dykeman	V 1.10
July 6, 2011	Karen Waite	Revised to remove ‘follow-up items’	V1.11
Nov 28, 2012	Karen Waite	Review and revision	V 1.12

2. Purpose

This policy outlines the context within which Healthtech Consultants (Healthtech) operates, and how it handles information in its custody and control. It sets general rules related to information management and provides its employees and contracted workers direction on how to protect confidential information, both during and after the employee or contracted worker's association with Healthtech. This policy is not intended to replace policies which have been approved by organizations to which Healthtech provides services. Healthtech acknowledges that its consultants, when providing services to a client, must respect the privacy framework of the client, including the legislation, regulations and policies to which the client organization is subject.

3. Introduction

Healthtech is committed to protecting the privacy, confidentiality and security of all confidential information to which it is entrusted, whether it is confidential corporate information; personal information (PI)[1]or personal health information (PHI)[2] (collectively, Confidential Information) which may be held by either a client or by Healthtech or to which Healthtech employees or contracted workers may have access during the course of a client engagement. Healthtech is a Canadian-based commercial enterprise serving the health care sector, primarily in the Canadian market. Its predominant business is providing consulting services to organizations which use, or are intending to use, information technology in the delivery or in the support of the delivery of care/services to the organizations' patients/clients.

From a privacy perspective, Healthtech, as a commercial enterprise which may collect personal information in the course of commercial transactions, is subject to the Personal Information Protection and Electronic Documents Act, Canada, 2000 (PIPEDA). However, it's important to note that PIPEDA does not govern personal information collected, used or disclosed about employees.

Further, in the course of conducting its work in the Canadian healthcare industry, Healthtech works with clients who may be subject to a number of privacy specific statutes and regulations or statutes and regulations which include privacy or confidentiality provisions. Each engagement, depending on its nature and geographic location, will require Healthtech employees and contracted workers to act according to legislation applicable in that particular jurisdiction, and to the particular circumstance.

Confidential Information and the legislation, regulation and policies which apply to it varies according to the ownership or custodianship of the information; who is accessing the Confidential Information; and under what circumstance it is being accessed. The table below provides guidance to Healthtech employees and contracted workers regarding where to seek guidance in particular circumstances.

---

[1] Personal Information defined by the Personal Information Protection and Electronic Data Act (PIPEDA) is: 'Information about an identifiable individual, but does not include the name, title, or business address or telephone number of an employee of an organization.'

[2] Personal Health Information defined in the Personal Health Information Protection Act, Ontario 2004 is

"... 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 *Home Care and Community Services Act, 1994* for the individual,

(d) relates to payments or eligibility for health care, or eligibility for coverage 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. 2004, c. 3, Sched. A, s. 4 (1); 2007, c. 8, s. 224 (6); 2007, c. 10, Sched. H, s. 2.

Table 1 – Confidential Information Framework

Who's Accessing	Types of Information being Accessed and Protected			Where is the Information Residing?	Which Data Protection Policies Apply?
Client Employees/Staff	Client Confidential Corporate Information (e.g. Financial)	Client Personal Information (e.g. Employee Benefits Records)	Client Personal Health Information (e.g. Health Card Numbers, Patient Records)	Client Site	Client Policies apply.
Healthtech Employee/Contracted Workers	Client Confidential Corporate Information (e.g. Financial)	Client Personal Information (e.g. Employee Benefits Records)	Client Personal Health Information (e.g. Health Card Numbers, Patient Records)	Client Site	Client Policies apply - **Healthtech Employees must comply with *Client's* Policies and Procedures.**
Healthtech Employee/Contracted Workers	Healthtech Confidential Corporate Information (e.g. proprietary methodology etc)	Healthtech Personal Information (e.g. Employee Benefits Records)	**Client** Confidential Information (Corporate, Personal Information, Personal Health Information)	Healthtech Site	Healthtech Policies apply – **Healthtech Employees must comply with *Healthtech* Policies and Procedures *and* *Client's* Policies and Procedures to the extent that**

					Client Confidential Information is being handled.

This policy is applicable to Healthtech employees, contracted workers, students or volunteers operating under the direction of Healthtech. This policy is not intended to provide direction to Healthtech clients regarding confidential information assets that they control.

4. Principles, Policies, and Procedures

Healthtech consultants provide services to many different organizations in different jurisdictions (federal, provincial, territorial and in the United States). Confidential Information of Healthtech's clients are subject to multiple (and sometimes inconsistent) legislative frameworks. This policy does not attempt to catalogue the various legislative frameworks governing privacy and confidentiality some of which are under development. If a Healthtech consultant is uncertain of the privacy obligations of a client to which they are providing services, it is incumbent on the consultant to direct their inquiries to the Privacy Officer affiliated with the client organization.

Regardless of the specific privacy legislative framework at play in a particular jurisdiction, the Organization for Economic Cooperation and Development (OECD) Guidelines for the Protection of Privacy and Transborder Flows of Personal Data are widely accepted as the principles upon which privacy best practice is based. The Canadian Standards Association (CSA) Model Code for the Protection of Personal Information builds on the OECD Guidelines and acts as the foundation PIPEDA as well as provincial privacy legislation in Canada. Canada Health Infoway's Privacy Blueprint and related privacy requirements are also based on the OECD/CSA principles.

CSA Model Code consists of ten privacy principles as follows:

- Accountability**;**
- Identifying Purpose;
- Consent;
- Limited Collection;
- Limiting Use, Storage and Disclosure;
- Accuracy of Information;
- Safeguards;
- Openness;
- Access; and
- Compliance.

As Healthtech is subject to PIPEDA, each of the principles outlined in Section 5, Schedule 1 of that Act have been reproduced in the following tables. Healthtech's policy statements with respect to each of the principles are articulated in the tables below.

4.1 Principle 1: Accountability

4.1.0	Accountability
'An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.	
4.1.1 Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).	
4.1.2 The identity of the individual(s) designated by the organization to oversee the organization's compliance	

4.1.0	Accountability

with the principles shall be made known upon request.

4.1.3

An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4

Organizations shall implement policies and practices to give effect to the principles, including

(*a*) implementing procedures to protect personal information;

(*b*) establishing procedures to receive and respond to complaints and inquiries;

(*c*) training staff and communicating to staff information about the organization's policies and practices; and

(*d*) developing information to explain the organization's policies and procedures.'[3]

Policy Statement

Healthtech acknowledges accountability for all Confidential Information, including personal information, under its control.

Accountability for Healthtech's compliance with the principles and policies contained within rests with President of Healthtech. Given that accountability, the President has final decision-making authority regarding the interpretation and application of the principles and policies, including disciplinary action when a breach of policy has taken place. The President of Healthtech has delegated day to day privacy activities to Healthtech's Privacy Officer.

The fact that Healthtech's President is accountable for its privacy practices is made explicit through this policy which is available to its employees and contracted workers through its internal SharePoint site and is available, on request, to external parties.

Healthtech enters into contractual relationships with its employees, contracted workers, clients and suppliers. Contracts negotiated with these parties refer to the party's respective obligations as it relates to the protection of Confidential Information assets.

Healthtech Senior Management is responsible for the development of an 'information-protection/conscious' organizational culture including the assignment of sufficient resources to support this development. This Privacy Policy is evidence of Healthtech's commitment to the protection of Confidential Information.

All new employees are expected to read the Privacy Policy as part of the orientation process, and to indicate their agreement with the Healthtech confidentiality agreement appended to this policy. The Policy is reviewed and all employees indicate their agreement with the Confidentiality Agreement on an annual basis thereafter.

See Appendix A.

[3] Principles set out in the National Standard of Canada entitled *Model Code for the Protection of Personal Information*, can/csa-q830-96 as referenced in Schedule 1, Section 5 of the Personal Information Protection and Electronics Document Act, Canada, 2000.

4.2 Principle 2: Identifying Purposes

4. 2.0	Identifying Purposes

'The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

4.2.1

The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle and the Individual Access principle

4.2.2

Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle requires an organization to collect only that information necessary for the purposes that have been identified.

4.2.3

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle.

4.2.5

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6

This principle is linked closely to the Limiting Collection principle and the Limiting Use, Disclosure, and Retention principle.'[4]

Policy Statement

Healthtech collects personal information from employees as is required for employment purposes – including the employees' home address in order to administer payroll and benefits programs. Healthtech discloses limited personal information to its contracted payroll administrator and discloses personal information to its benefits administrator as required.

Healthtech's website includes functionality for individuals to submit a request to contact Healthtech should they have an inquiry. In this instance, individuals provide contact information which may include name, e-mail address, and telephone number to Healthtech so that a representative of Healthtech may respond to the request for information. Healthtech uses the information to respond to the request and does not use this information for any other purpose.

Healthtech has documented the purposes for the collection of personal information in this privacy policy which is available to employees. This policy is available on request to external parties.

Healthtech limits collection of personal information to that which is required for the purpose.

Healthtech also documents the purpose for the collection of information on the forms that it uses

[4] Principles set out in the national standard of Canada entitled *model code for the protection of personal information*, can/csa-q830-96 as referenced in Schedule 1, Section 5 of the Protection of Personal Information Protection and Electronics Document Act, Canada, 2000

4. 2.0	Identifying Purposes

to collect that information.

It is Healthtech's policy to notify individuals of its intention to collect new information for a new purpose or to use existing information for a new purpose that goes beyond that which has been communicated through this policy.

4.3 Principle 3: Consent

4.3.0	Consent

'The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2

The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

4.3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.0	Consent

4.3.7

Individuals can give consent in many ways. For example:

(*a*) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(*b*) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(*c*) consent may be given orally when information is collected over the telephone; or

(*d*) consent may be given at the time that individuals use a product or service.

4.3.8

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.'[5]

Policy Statement

While not subject to PIPEDA as it relates to personal information about its employees, Healthtech acknowledges employee's right to know what information is being collected, how the information is being used and to whom the information is being disclosed. Healthtech considers consent having been obtained from the individual when the individual completes the necessary forms and provides necessary information when signing up for payroll administration and benefits. Individuals may withdraw their consent for the collection or disclosure of personal information as it relates to payroll and benefits and the individual may consult with Healthtech's Privacy Officer or Payroll and Benefits administrator to determine the impact of the withdrawal of consent for the collection or disclosure of personal information and to make arrangements to withdraw consent.

4.4 Principle 4: Limiting Collection

4.4.0	Limiting Collection

'**The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.**

4.4.1

Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle.

4.4.2

The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3

This principle is linked closely to the Identifying Purposes principle and the Consent principle.'[6]

[5] Principles set out in the national standard of Canada entitled *model code for the protection of personal information*, can/csa-q830-96 as referenced in Schedule 1, Section 5 of the Protection of Personal Information Protection and Electronics Document Act, Canada, 2000

[6] ibid

4.4.0	Limiting Collection

Policy Statement

Healthtech limits the collection of personal information to that which is required to fulfill the purposes of administering payroll and the benefits program. It does not collect personal information indirectly but rather directly from the individual with their knowledge and consent.

4.5 Principle 5: Limiting Use, Disclosure and Retention

4.5.0	Limiting Use, Disclosure and Retention

'**Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes**.

4.5.1

Organizations using personal information for a new purpose shall document this purpose.

4.5.2

Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3

Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4

This principle is closely linked to the Consent principle, the Identifying Purposes principle and the Individual Access principle.'[7]

Policy Statement

Healthtech limits use and disclosure of personal information to that which is required to fulfill the purposes and for the purpose for which it has been collected. Any new purposes are documented and individuals are made aware of this new purpose so that they may provide consent. Information which is no longer required to fulfill the purpose is disposed of securely.

4.6 Principle 6: Accuracy

4.6.0	Accuracy

'Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

4.6.1

The extent to which personal information shall be accurate, complete, and up-to-date will depend upon

[7] Principles set out in the National Standard of Canada entitled *Model Code for the Protection of Personal Information*, can/csa-q830-96 as referenced in Schedule 1, Section 5 of the Personal Information Protection and Electronics Document Act, Canada, 2000.

4.6.0	Accuracy

the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

4.6.2

An organization shall not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.

4.6.3

Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.'[8]

Policy Statement

Healthtech requires its employees to provide updated information so as to ensure that the personal information it has on record is accurate. Healthtech does not, as a matter of policy, update information on behalf of employees as it would not independently hold nor have access to information of the nature that would require updating (e.g. change of personal phone number or address).

4.7 Principle 7: Safeguards

4.7.0	Safeguards

'Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.

4.7.3

The methods of protection should include

(*a*) physical measures, for example, locked filing cabinets and restricted access to offices;

(*b*) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and

(*c*) technological measures, for example, the use of passwords and encryption.

4.7.4

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.'[9]

[8] Principles set out in the National Standard of Canada entitled *Model Code for the Protection of Personal Information*, can/csa-q830-96 as referenced in Schedule 1, Section 5 of the Personal Information Protection and Electronics Document Act, Canada, 2000.

4.7.0	Safeguards

Policy Statement

Healthtech is committed to ensuring the confidentiality, integrity, availability of information assets entrusted to it. Healthtech's Security Policy is under development and will detail its security practices. All Healthtech employees will be required to comply with it.

4.8 Principle 8: Openness

4.8.0	Openness

'An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1

Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2

The information made available shall include

(*a*) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;

(*b*) the means of gaining access to personal information held by the organization;

(*c*) a description of the type of personal information held by the organization, including a general account of its use;

(*d*) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and

(*e*) what personal information is made available to related organizations (e.g., subsidiaries).

4.8.3

An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.'[10]

Policy Statement

This policy details Healthtech's privacy practices and is available to employees through the organization's SharePoint site. It is also available, on request, to third parties as requested. Requests may be directed to Healthtech's President or to Healthtech's designated Privacy Officer.

[9] Ibid

[10] Principles set out in the National Standard of Canada entitled *Model Code for the Protection of Personal Information*, can/csa-q830-96 as referenced in Schedule 1, Section 5 of the Personal Information Protection and Electronics Document Act, Canada, 2000.

4.9 Principle 9: Access

4. 9.0	Access

'**Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.**

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

4.9.1

Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.2

An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

4.9.3

In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

4.9.4

An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

4.9.5

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

4.9.6

When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.[11]

Policy Statement

Healthtech acknowledges the right of individuals to have access to their personal information

[11] Principles set out in the National Standard of Canada entitled *Model Code for the Protection of Personal Information*, can/csa-q830-96 as referenced in Schedule 1, Section 5 of the Personal Information Protection and Electronics Document Act, Canada, 2000.

4. 9.0	Access
held by Healthtech. Any employee who wishes to access their personal information collected, retained or disclosed by Healthtech can make their request via e-mail to Healthtech's Privacy Officer.	

4.10 Principle 10: Compliance

4.10.0	Compliance

'**An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.**

4.10.1

The individual accountable for an organization's compliance is discussed in Clause 4.1.1.

4.10.2

Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

4.10.3

Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

4.10.4

An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.'[12]

Policy Statement

Any individual who has an inquiry about Healthtech's information management practices shall direct their inquiry in writing to either Healthtech's President or Privacy Officer. As per PIPEDA complaints associated with personal information collected for commercial use may be lodged with the Federal Information Privacy Commissioner by completing a form which can be found at the following link. http://www.priv.gc.ca/I_I/form_e.cfm#contenttop . Complaints must be mailed to:

Office of the Privacy Commissioner of Canada
Place de Ville, Tower B
3rd Floor
Ottawa, ON K1A 1H3
Fax: 613-947-6850
Inquiries: Toll Free #: 1-800-282-1376

[12] Ibid.

5. Provincial Privacy Legislation - Ontario

There are a number of provincial statutes and regulations which prescribe the manner in which personal and personal health information is to be managed in those jurisdictions. Legislative frameworks in each of the jurisdictions are evolving as each jurisdiction comes to terms with the need to prescribe information handling practices. Generally speaking, most provinces have enacted statutes which allow citizens to access records from public institutions which also protect personal information assets at these organizations. These are generally called 'Freedom of Information and Protection of Privacy Acts' with an acronym of FIPPA or FOIPPA. The reason to highlight this type of legislation is to ensure that Healthtech employees/consultants are aware that records created as part of the relationship between Healthtech and the public organization (including correspondence and contracts) may be subject to Freedom of Information Access Requests and therefore become public. The degree to which Healthtech may be exposed to this may vary from one jurisdiction to another.

Some, but not all, jurisdictions in Canada have proclaimed ***health sector specific*** privacy legislation. Health sector specific privacy legislation may have an impact on how personal health information is to be handled at client sites. Prince Edward Island, Northwest Territories, Nunavut and the Yukon do not yet have health sector specific privacy legislation.

Healthtech employees and consultants are not expected to be subject matter experts in privacy legislation across multiple jurisdictions; however, they must be aware that legislation may have an impact on their information management practices. As previously indicated, client organizations are obliged to provide direction with respect to applicable legislation and specific policies to Healthtech consultants when consultants are providing services on their behalf. That said, it is incumbent on Healthtech consultants to be vigilant and ask appropriate parties questions should uncertainty arise. This is further delineated in policy statements to follow. Below please find background and highlights from some, but not all of the provincial statutes as well as policy statements associated with them.

ONTARIO

Public organizations in Ontario are subject to two privacy statutes which are described below.

Personal Health Information Protection Act, Ontario, 2004 and ***PHIPA Regulation 329/04***.

Generally, this statute and associated regulation provides direction to organizations and individuals known as Health Information Custodians (HIC) for the handling of Personal Health Information (PHI). Healthtech and its consultants could potentially play a number of PHIPA roles at the direction of the Health Information Custodian procuring Healthtech services, depending on the circumstance. These roles include PHIPA Agent, and Service Provider. These roles limit Healthtech and Healthtech consultants to collecting, using, disclosing and handling personal health information in the manner that PHIPA requires of the HIC.

Policy Statement

Healthtech consultants providing services to healthcare organizations in Ontario are referred to the Privacy Officer employed at the client site for direction as to the client's expectations for information management practices. Should the Healthtech employee have a question concerning their role which cannot be brought or is inappropriate to bring to the client Privacy Officer, the Healthtech employee will direct their question to the Healthtech Privacy Officer.

Healthtech Employees will not access Personal Health Information from an Ontario site without the express, written request from the Health Information Custodian for the PHI at issue. Healthtech employees accessing PHI will do so on the Client Site or remotely

through the Client Site VPN and shall not, under any circumstances save, store or otherwise remove PHI from the client site without express, written authorization from Healthtech's Privacy Officer. On authorization to do so, this will be done subject to the conditions outlined, in writing, by the Privacy Officer.

Further, at any time a Healthtech Employee has accessed or been provided with Personal Health Information which has not been explicitly authorized, the Healthtech Employee must immediately notify the Privacy Officer of the Ontario client site associated with the PHI and Healthtech's Privacy Officer.

Freedom of Information and Protection of Privacy Act, **Ontario, 1990 (FIPPA)**.

This statute requires designated public institutions (including the Ministry of Health and Long-Term Care, eHealth Ontario, Universities and, as of January, 2012, all public hospitals in Ontario) to provide access to personal information upon request. The Act protects personal information from being released, however, subject to limited exemptions, all other records are subject to release. This is important for Healthtech as any correspondence, including contracts, invoices, work products, e-mail or voice-mail messages may be subject to release.

Policy Statement

Healthtech employees, when corresponding with organizations subject to FIPPA shall create records with the understanding that they are not necessarily private – that is, shall ensure that all correspondence is professional, reflects well on both the employee and the organization. Should Healthtech employees have questions about information management practices as it relates to FIPPA, they should consult with Healthtech's Privacy Officer.

6. Privacy Legislation – Outside Ontario

Policy Statement

Healthtech Consultants working outside of Ontario and who have questions about the way in which privacy legislation may impact their engagements should seek direction from their clients, preferably the Privacy Officer, if any, at the client site. Any unresolved questions or concerns can be brought to the attention of Healthtech's Privacy Officer.

7. Privacy and Security Incidents/Potential Incidents

In the course of their duties, Healthtech employees may come across an actual or potential unauthorized disclosure of Confidential Information. Should this occur, it is incumbent on the employee to report this occurrence, as it may be required by legislation or policy and/or may assist in preventing a serious situation from occurring in the future. Healthtech's Privacy Incident Policy and associated Procedure will provide employees with direction. Employees are required to read the policy and procedure and to direct any questions to Healthtech's Privacy Officer should any questions arise.

Policy Statement

If any Healthtech employee experiences a potential or actual privacy or security incident or breach the employee will follow Healthtech's Privacy and Security Incident Management Policy and Procedure.

References:

The following sources were used as reference documents to develop the corporate policy for Healthtech Consultants:

- COACH Guidelines for the Protection of Health Information – December 2006;
- Electronic Health Record Privacy and Security Requirements, Canada Health Infoway, V1.1;
- Canadian Standards Association (CSA) Model Code for the Protection of Personal Information (CAN/CSA-Q830-96);
- Fact Sheet, January 2005, Safeguarding Personal Information, Information and Privacy Commission of Ontario, http://www.ipc.on.ca/english/Resources/Educational-Material/;
- Fact Sheet, June 2007, Wireless Communication Technologies: Safeguarding Privacy and Security, Information and Privacy Commission of Ontario, http://www.ipc.on.ca/english/Resources/Educational-Material/ ; and
- Fact Sheet, May 2007, Encrypting Personal Health Information on Mobile Devices, Information and Privacy Commission of Ontario, http://www.ipc.on.ca/english/Resources/Educational-Material/.

Appendix A:

Confidentiality Agreement

Appendix A: Confidentiality Agreement

Healthtech Consultants ("Healthtech") is committed to protecting individual privacy and the confidentiality and security of information it holds in order to provide services and in the normal course of business. This information may include personal information, personal health information (PHI), and/or corporate information (financial, payroll, human resources information and/or any other proprietary information) held by Healthtech or by our clients on Healthtech premises or at a client site, and is called "Confidential Information" for purpose of this agreement.

This AGREEMENT must be acknowledged and agreed to by all employees and contractors annually.

In my capacity as a Healthtech employee or contractor, I understand and agree as follows:

- I acknowledge that I have read and understood Healthtech's Privacy Policy;
- I will comply with the Healthtech Privacy Policy and all related privacy policies and procedures;
- I will not access or use any Confidential Information that I learn of or possess in my role at Healthtech, unless it is necessary for me to do so in order to perform my job responsibilities;
- If PHI is transmitted to me I will contact the Healthtech Privacy Officer and Technical Advisor immediately for follow-up and investigation.
- I will not disclose or discuss Confidential Information except to other persons who are authorized to receive such information;
- I will not alter, destroy, copy or interfere with Confidential Information, except with authorization and in accordance with the policies and procedures;
- I agree to adopt appropriate physical and technical safeguards for Confidentiality Information, including keeping any computer access codes (for example, passwords) confidential and secure and protecting physical access devices (for example, keys and badges). I will not lend my access codes or devices to anyone, nor will I attempt to use those of others; and
- I understand that alleged breaches will be investigated.

I **acknowledge** that my failure to comply with the above, or my participation in a breach of privacy, may result in disciplinary action. By entering into this agreement, I acknowledge that this agreement continues in effect even once my employment or affiliation with Healthtech ends.

By responding "I accept" to the e-mail which includes the Privacy Policy and this AGREEMENT, your acknowledgement, understanding and agreement to the above will be confirmed.