CANADIAN HEALTH INFORMATION MANAGEMENT ASSOCIATION

Corporate Privacy Code

Revised: February 2018

Table of Contents

Introduction

The Canadian Health Information Management Association (CHIMA) provides a wide range of health information management services to its members and other health care stakeholders across Canada.

To demonstrate its commitment to implement appropriate safeguards CHIMA has developed a comprehensive Information Protection Program. The program will:

- Protect the privacy of personal information in the possession of CHIMA;
- Minimize the risk of unauthorized access, use or disclosure of personal information;
- Articulate staff obligations with respect to information protection and outline consequences of security breaches;
- create an organizational culture of secure behaviours; and
- demonstrate CHIMAs commitment to its members in this regard and openness to public review

The Privacy Code is one component of the Information Protection Program. It outlines corporate initiatives and individual responsibilities for protecting personal information and underscores a fundamental principle of information protection; each of us has a responsibility to protect personal information.

It is important to define some terms used throughout this document to ensure that there is a common understanding of key concepts. Information protection encompasses privacy, confidentiality and security issues. These terms are often used interchangeably although there are some important distinctions.

Privacy refers to the right of a person to control who has access to their personal information and under what circumstances.

Confidentiality refers to a third party's obligation to ensure that only authorized users have access to personal information. In other words, confidentiality speaks to organizational responsibilities while privacy refers to individual rights.

Security is characterized as the preservation of the confidentiality, integrity, and availability of personal information. Information security is achieved by putting into place relevant physical, technical and organizational policies, procedures and measures.

Personal information is defined as information in any form about an identifiable individual or group such as:

- the name, position title
- Information pertaining to an identifiable individual who is an applicant for or is a current or past member of CHIMA.
- Mandatory Information for Certification and enrollment in the College of Health Information Management (CCHIM)
- Continuing Professional Education (CPE) information
- Member services information in the CHIMA database.

Core demographic and administrative information that CHIMA requests to provide services include:

-Name (first and last)
-Date of Birth
-Mailing Address
-Home Telephone
-Email Address
-Methods of Payment
-Credit Card Account Number when this method of payment is selected
-Organization
-Position/Title
-Work Telephone
-Work Facsimile Number

CHIMA Website - CHIMA tracks visitors to their public website for statistical purposes. The site captures limited information about visits. No personally identifiable information is collected, only aggregate data - such as the number of hits per page.

For members only web pages accessible by authorized members, names of the members, email addresses and passwords are collected to authenticate levels of access and track the number of times members have visited the site.

CHIMA is not responsible for the content or privacy practices of any linked site.

Data uses - CHIMA uses information submitted from members, conference registrants, and other customers in the following ways:

- To improve its Web content;
- To respond to members' and visitors' interests, needs and preferences;
- To develop new products and services; and
- To provide individuals and companies with information about complimentary CHIMA services, promotions or special offers.

Aggregate data are used only to analyze general traffic patterns (e.g. what pages are most/least popular) and to perform routine system maintenance.

Data sharing - CHIMA member data is never disclosed beyond the organization without the consent of the Member and it is shared internally only when it is required as a part of the performance of the duties of the individual seeking access.

Member-in-Good-Standing (Name/Province) is listed on the website (certification information).

CHIMA does not make members' contact information available through the CHIMA Membership Database to third parties or visitors to its Internet site but does make it available, with appropriate consent.

CHIMA may elect to send mailings from other organizations to its members, with the approval of the Chief Executive Officer of CHIMA, but the mailings will always originate with CHIMA.

If a member chooses to contact CHIMA by mail, fax, telephone or email, and provides personally identifiable information, CHIMA does not use the information for any purpose other than to respond to the member inquiries.

CHIMA does not retain credit card account information provided by its members and customers to the appropriate banking institutions and/or clearinghouses in order to obtain debit authorization and payment. Credit card information is retained at Executive Office for all faxed or phoned payments, for authorization purposes.

Canadian Health Information Management Association (CHIMA) provides information management services to clients in industries which include compliance with national, provincial and territorial privacy legislation across Canada.

In providing these services, CHIMA recognizes its obligation as an agent of the client, to take all reasonable steps to protect the privacy and security of any personal information accessed or used by any CHIMA employee, sub-contractor or third party agent.

Privacy and security obligations will be identified and articulated as part of each Service Level Agreement and/or Data Sharing Agreement as required by each client.

As part of this obligation to its clients, and in compliance with national, provincial and territorial legislation, CHIMA has adopted and included the "Principles of Best Practice" as developed by the Canadian Standards Association (CSA) as follows:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

These are based upon international guidelines, form the basis of most privacy legislation in Canada and include the Federal 'Personal Information Protection & Electronics Document Act' (PIPEDA). In the absence of any specific national, provincial or territorial legislative requirements, the Federal legislation will be followed.

Statement

The Privacy Officer shall be designated as the representative for CHIMA. The Privacy Officer is the CEO of CHIMA. The Privacy Officer is authorized to act for CHIMA in all issues pertaining to policies and procedures regarding privacy and confidentiality for personal information. This role applies to personal information obtained and used as part of the contractual service level agreements, data sharing agreements as well as policies/procedures for CHIMA's corporate personal information relating to employees, subcontractors and service suppliers.

Procedure

The Privacy Officer will post the Privacy Statement on public forums, including public office areas, brochures, websites and other media, designed to inform CHIMA's customers, clients and the public.

The Privacy Officer shall have sufficient authority within CHIMA to act and communicate on the company's behalf and have full authority to comply with National, Provincial and Territorial legislation requirements (Refer to Privacy Breach Checklist).

The Privacy Officer will deal with all privacy of personal information issues, privacy breach incident management, investigate and address complaints as required by CHIMA policies, procedures and legislative requirements.

The Privacy Officer will collaborate with clients and organizations to address, correct and prevent any recurrence, as well as recover any unauthorized disclosure of personal information, as a result of any notice of breach procedures.

The Privacy Officer will update policies and procedures as may be required by changes to privacy and information legislation.

The Privacy Officer is responsible for the education and training of all employees regarding information privacy and confidentiality policies, procedures and security procedures as part of their initial employment and incorporated in the annual review process for each employee.

The Privacy Officer will administer and maintain employee, suppliers and subcontractors' signed pledges of confidentially and make these available to clients if required under any service provision contracts, service level agreements or data sharing agreements.

The Privacy Officer shall conduct periodic inventory of data holdings and ensure compliance with retention, disposal, security and other policies/procedures for protection of personal information used by CHIMA.

The Privacy Officer shall provide information regarding CHIMA's privacy protection policies/ procedures and participate in any Threat/Risk Assessments and Privacy Impact Assessments as may be required by CHIMA's clients and their organizations.

CHIMA organization will designate the Privacy Officer responsible for security coordination, allocation of information security responsibilities, confidentiality agreements, independent review and managing risks related to third parties.

Overarching Policy Statements:

C.1 – ACCOUNTABILITY:

1. CHIMA will perform its services in a professional manner, in accordance with industry standards and practices, by properly trained employees.
2. CHIMA provides services to its clients as an agent of the client and as such, complies with National, Provincial and Territorial legislation as permitted or required and at the direction of the client.
3. CHIMA's employees understand that breach of the security and confidentiality of their clients' personal information may lead to disciplinary measures.
4. If CHIMA engages the services of a third party to perform all or part of the services under a contract, CHIMA shall inform the client prior to and within the contract agreements and negotiations.

C.2 – IDENTIFYING PURPOSES:

1. CHIMA shall use any personal information accessed, used, collected only as necessary for purposes of performance of responsibilities relating to corporate and business requirements, administration of employee and human resources as well as providing service contract obligations to clients and identified under any service level provision or data sharing agreements.
2. Personal Information as described in CHIMA's policies will also include Personal Health Information as defined as *information about an identifiable individual that relates to the physical or mental health of the individual, or provision of health services to the individual, and may include:*
   - *information about the registration of the individual for the provision of health services,*
   - *information about payments or eligibility for health care in respect to the individual,*
   - *a number, symbol or particular assigned to an individual to uniquely identify the individual for health care purposes,*
   - *any information about the individual that is collected in the course of the provision of health services to the individual, and*
   - *information derived from the testing or examination of a body part or bodily substance*
3. CHIMA shall ensure that any third party supplier, vendor or subcontractor adheres to this requirement.
4. The Purposes for which the information will be used, accessed or collected by CHIMA will be stated and agreed to in contracts with CHIMA clients and extended to third party suppliers, subcontractors and vendors.

C.3 – CONSENT:

1. CHIMA acts as an agent for its clients and the client will maintain full authority over issues of consent for management including disclosure of personal information. CHIMA will not act independently regarding consent issues unless at the specific case by case basis at the direction of the client organization.

2. Specific direction regarding consent must be included in each service provision agreement, service level agreement and/or data sharing agreement.

3. CHIMA acknowledges that consent may be withdrawn by an individual and CHIMA will work with clients to the best of their ability to assist in compliance with legislative provisions.

C.4/5 – LIMITING COLLECTION, USE, DISCLOSURE & RETENTION:

1. CHIMA will collect, use, disclose and retain personal information only for purposes to fulfill obligations defined in service provisions, client contracts and as required by legislation.

2. CHIMA will disclose information to authorized users only as identified and agreed upon with clients under service provision contracts.

3. CHIMA's role in disclosure of personal information as collected for and from clients is contained as a vendor/supplier to the client only. Disclosure of personal and other information must be under the control and direction of the client.

4. CHIMA shall not disclose any personal information for 'secondary uses' to other third parties unless directed by the client and/or as required by Canadian law or court order. (Note: Secondary purposes are generally considered purposes that are not directly related to the care and treatment of a patient, heath research, health system planning, quality assurance, conducting health service provider education and health policy development as examples)

5. CHIMA will retain any personal information collected or used for purposes of service provision obligations only for as long as required to fulfill those obligations and/or as required by National, Provincial or Territorial legislation.

6. CHIMA will return and/or destroy any personal information collected or used for purposes of service provision obligations as authorized and directed by the client upon completion of the contracted service.

C.6 – ACCURACY

1. CHIMA will make every effort to ensure services that are provided as described in service level agreements and contracts are accurate and complete.

2. CHIMA will comply with national, provincial and territorial legislation and at the direction of client, correct, change or modify records that are under the control of the client (as the custodian) but currently residing physically or electronically with CHIMA.

3. CHIMA will validate the identity of any persons or system requesting correction or change and only after proper authorization from the client as may be described in contracts or data sharing agreements.

4. CHIMA will comply with requests for investigation of complaints or suspected Breach of Privacy activities as required by their clients.

C.7 – SAFEGUARDS & SECURITY:

1. CHIMA will maintain this Policy for the Protection of Personal Information and review/revise as is necessary for Safeguards and Security for management of personal information.

2. CHIMA organization will designate the Privacy Officer responsible for security coordination, allocation of information security responsibilities, confidentiality agreements, independent review and managing risks related to third parties;

3. CHIMA will ensure security measures for asset management including information asset inventories, ownership, and acceptability other required procedures and handling;

4. CHIMA will ensure human resources security, including screening prospective workers prior to employment, outlining terms and conditions of employment, outlining management responsibilities, conducting information security awareness and education, establishing a disciplinary process and the removal of access rights and return of assets upon termination of employment;

5. CHIMA will ensure physical security, including physical security perimeters and entry controls, securing work areas and facilities, protecting against environmental threats and failures, working in secure areas, public access, the privacy-protective positioning of equipment such as monitoring equipment, maintenance and protection off-premises, secure disposal or reuse of equipment and removal of property;

6. CHIMA will ensure security in communications and operations management, including operational procedures and responsibilities, third party service delivery management, system planning and acceptance, protection against malicious and mobile code (malware), back-up, network security management, media handling (managing and disposal of removable media), and information exchange policies, procedures and agreements (including physical media in transit and electronic messaging);

7. CHIMA will ensure security for access control to each of its systems, applications and databases, including establishing an access control policy, user access management (registration, privilege management, authentication mechanisms), user responsibilities, network access control, and operating system access control, including access to all mobile computing and teleworking technologies;

8. CHIMA will include security procedures as outlined in policies/procedures during information systems acquisition, development and maintenance, including specification of security requirements in information systems, integrity controls in applications, cryptographic controls, security of system files, security in system development and support processes and technical vulnerability management;

9. CHIMA will implement information security incident management procedures as required by national, provincial, and territorial legislation including information security incident reporting and managing security incidents and improvements (procedures, learning from incidents and collection of evidence); and

10. CHIMA will implement information security aspects of business continuity management, including business continuity and risk assessment, developing and implementing continuity plans and testing, maintaining and reassessing plans.

C.8 – OPENNESS:

CHIMA will make policies and procedures readily available to clients and the public by:

1. Posting CHIMA's Privacy Statement in the public domain, offices, on websites and other locations accessible to clients and the public
2. Providing the name and contact information of CHIMA's Privacy Officer to enable any privacy/confidentiality issues to be addressed within legislative timeframes
3. Providing clients with personal information held on clients' behalf to those clients
4. Providing authorized access to clients for whom CHIMA acts as their agent

C.9 – INDIVIDUAL ACCESS:

1. CHIMA will grant access to personal information only to authorized persons as stated within contracts with clients.

2. Individuals will only access personal information which is held by CHIMA on behalf of clients for the fulfillment of their duties as identified in contracts for service provision and as authorized by their level of access.

C.10 – CHALLENGING COMPLIANCE:

1. CHIMA will provide contact and complaint procedure information for anyone wishing to challenge compliance with company privacy policies or national, provincial and/or territorial legislation.

2. CHIMA will post the Privacy Officer name, contact information, email address, phone number as well as the provincial privacy commissioner's name, contact information, email address and phone number on public brochures, websites or other media to enable communication regarding any privacy issues or complaints.

3. CHIMA Privacy Officer will investigate any complaints within timeframes as identified in national, provincial and territorial privacy legislation.