Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

# Privacy Classification of Health Information in Alberta – Issues, Proposed Solution and Benefits

by

VIEGAS, Edwina

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

**Date: April 2008**

Research advisors:

Ron Ruhl, Director and Associate Professor, MISSM

Andy Igonor, Associate Professor, MISSM

# Privacy Classification of Health Information in Alberta – Issues, Proposed Solution and Benefits

by

VIEGAS, Edwina

Research advisors:

Ron Ruhl, Director and Associate Professor, MISSM

Andy Igonor, Associate Professor, MISSM

Reviews Committee:

Andy Igonor, Assistant Professor, MISSM
Dale Lindskog, Assistant Professor, MISSM
Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

**Date: April 2008**



**The author acknowledges the significant contributions to the work by Academic Advisors and Review Committee Members and gives the right to Concordia Univeristy College to reproduce the work for the Concordia Library, Concordia Websites and Concordia MISSM classes.**

Concordia University College of Alberta, Edmonton

Information System Security Management (ISSM) 571

Research Paper

April 12, 2008

---

# Privacy Classification of Health Information in Alberta

# – Issues, Proposed Solution and Benefits

---

by

**Edwina Viegas**
Telephone: 780 464 1989
Email: viegasfamily@shaw.ca

**Research Advisors:**
Ron Ruhl
Assistant Professor and Director of the Information Systems Security Management Program
Concordia University College of Alberta

Andy Igonor
Assistant Professor, Information Systems Security Management Program
Concordia University College of Alberta

**Subject Matter Advisors:**
Wendy Robillard
Senior Manager, Health Information Policy and Compliance Unit, Alberta Health & Wellness

Brian Hamilton
Portfolio Officer, Office of the Information and Privacy Commissioner, Alberta

# TABLE OF CONTENT

# 1 ABSTRACT

This research paper reviews issues, proposes a solution and discusses the benefits of privacy classification for health information in Alberta. After a review and analysis of privacy classification of health information in Canada and the United Sates of America, this paper builds on existing privacy best practices and other work already completed. It recommends that by linking privacy classification guidelines with corresponding security classification guidelines and appropriate safeguards, privacy protection requirements could be made easy to understand and act upon. In addition, including appropriate definitions in the Alberta Health Information Regulation could have a positive impact by enforcing privacy protection and creating greater public confidence that their health information is protected.

# 2 INTRODUCTION

While Alberta's Health Information Act provides much rigour around the collection, use and disclosure of 'individually identifying health information', the definition and rules for 'non-identifying health information' appear to be ambiguous. With today's advanced technological tools and information sources available for data matching and data mining, there is uncertainty about what is really meant by non-identifying information, resulting in perhaps inappropriate safeguards being applied to the information. Because of this ambiguity, health organizations err on the side of caution and sometimes go above and beyond the controls required to protect the information, causing delays or restrictions in information sharing. Researchers or external requestors of information, unaware of the sensitivity of the information, or the appropriate privacy classification, expect a less stringent approach to information disclosure. As a result, their expected timelines are not met and their results sometimes become unachievable, with much time, energy and money wasted. A delay in timely research, could effect innovation and ultimately patient treatment and care.

The concerns expressed above have lead to this research with the following study objectives:

- To develop privacy classification guidelines for health information in Alberta and link it with corresponding security requirements and safeguards. This could complement the existing processes to enhance overall privacy protection, and could inform a revision to the Alberta health information legislation.
- To enhance the legislated health information privacy protection requirements with an Alberta Health Information Regulation including clarifying definitions to assist with privacy classification. This could make privacy protection requirements easy to understand, to communicate, and to act upon.
- To provide preliminary guidance on implementing the privacy classification guidelines to facilitate health information assessment and protection.

# 3 ORGANIZING THE STUDY

The study has been organized into two main sections:

- A review of the Health Information Act privacy classification and existing issues.
- The need for interconnectivity between privacy and security. This helps to justify the subsequent analysis of privacy classification and security classification, and ultimately the linking of the two to arrive at the proposed solution.

## 3.1 ALBERTA'S HEALTH INFORMATION ACT

Alberta's Health Information Act was proclaimed on April 25, 2001. The Act applies mainly in the publicly funded health sector, to "custodians" of health information, and their "affiliates" as defined in sections 1(1)(f) and 1(1)(a) of the Act.

The Health Information Act and regulations made under it establish rules that must be followed for the collection, use and disclosure of health information for those in the health system as well as the general public. The rules help to protect an individual's privacy and the confidentiality of their health information; ensure that their health information is shared appropriately; and that health records are managed and protected properly. (Health Information Act Guidelines and Practices Manual section 1.3)

The following are some of Alberta health information legislation's privacy enhancers or barriers to restrict the flow of information:

1. Custodians as trusted gatekeepers of information.
2. Consent for the disclosure of information.
3. Least amount of information to achieve the intended purpose.
4. Highest degree of anonymity possible in the circumstances.
5. Disclose for a role-based need-to-know.
6. Duty to protect the information in transit.
7. Periodic assessment of health information administrative, technical and physical safeguards.
8. Privacy Impact Assessments to the Information and Privacy Commissioner for review and comment.
9. Notation of disclosure indicating what was disclosed, why, when and to whom.
10. Offences or fines for unauthorized access to health information.

### 3.1.1 Alberta Health Information Privacy Classification and Issues

The Alberta Health Information Act defines the term health information [section 1(1)(k)] and also defines types of health information, i.e., registration information [section 1(1)(u)]; health services provider information [section 1(1)(o)]; diagnostic treatment and care information [section 1(1)(i)]. However, the privacy level categories or privacy classification of health information appear to be problematic. The Act classifies health information into the following privacy classification that is subjective and broad in scope: individually identifying information, non-identifying information, and aggregate information.

The Health Information Act section 1(1)(p) defines **individually identifying information** to mean "the identity of the individual who is the subject of the information can be readily ascertained from the information".

The Health Information Act section 1(1)(r) defines **non-identifying information** to mean "the identity of the individual who is the subject of the information cannot be readily ascertained from the information".

In the Health Information Act section 57(1) **aggregate health information** is defined as non-identifying health information about groups of individuals.

Several issues with the existing privacy classification have been identified below:

**Definitions:** The Health Information Act defines identifying and non-identifying information in terms of identity being "readily ascertainable". This is subjective and causes confusion as it pertains not merely to whether the information contains unique identifiers or not. It pertains to the entire range of elements in the information set.

**Potential Identifiers:** Without any identifiers present, a small data cell, e.g., 5 or less elements, could sometimes identify an individual, e.g., postal code in a rural area where less than five people reside.

**Safeguards:** Individually identifying health information appears to be protected by several stringent provisions in the health information legislation, e.g., privacy enhancers in section 3.1 of this paper. Rules for non-identifying information appear to be ambiguous, as the Act permits the custodian to collect, use and disclose this information for **any purpose**.

**Clarity:** With today's advanced technological tools and information sources available with or without a price for data matching and data mining, there is uncertainty about what is really meant by non-identifying information. How is the information made non-identifying, particularly before disclosure? This means different things to different people and accounts for variations in practices.

**Re-identification:** Lucock (2005) asks whether non-identifying information is sufficiently anonymized to exclude it from information protection legislation, including risks associated with incorrectly assuming that the information is not re-linkable. Section 32(2) of the Act merely states that if non-identifying information is disclosed to a non-custodian, the recipient must be advised to notify the Information Privacy Commissioner if the non-custodian wishes to use the information for data-matching.

**Anonymization:** While some information can be made non-identifying quite easily when it pertains to a limited period of time, it is difficult to anonymize longitudinal records that link patient lifetime health services encounters, as they could highlight patient patterns and eventually identify the patient e.g., monthly management statistics of the number of surgical procedures.

**Service Delivery:** After reading the Health Information Act, requestors of information could consider the information they request to be non-identifying. They could expect a less stringent approach to information disclosure. Health organizations err on the side of caution. When in doubt about the privacy classification of the information requested, they treat the information as individually identifying information, and sometimes go above and beyond the controls required to protect that information. As a result, the requestor's expected timelines may not be met and their results sometimes become unachievable, with much time, energy and money wasted, and perhaps important health outcomes compromised.

**Recommendation:** A granular, well defined privacy classification of health information in the legislation could ensure greater privacy protection by making the Health Information Act easier to understand, to administer and to audit.

### 3.1.2 Illustrating Scenario

This scenario describes some of the problems encountered with a request for information, and highlights the need for effective privacy classification guidelines for health information in Alberta.

Researcher R has developed a patient care assessment tool that is patented and can be used only by R and his team. R would like to assist health Custodian C by using the new tool and providing C with a patient care analysis that C would not be able to obtain otherwise. R believes that C could benefit from the analysis and recommendations, and ultimately be able to provide better care to their patients. R has provided a research proposal to C and has completed all the required paperwork for a request for what R believes to be non-identifiable information, which can be disclosed for any purpose.

C examines the information request and notes that R has requested certain patient care data elements for the last three years, including: Postal code, an encrypted or meaningless identifier, gender, age, and medications used by the patient. C considers the information requested to be individually identifying, as the full postal code, gender, age and medications used by the patient could easily identify the individual. For example, in rural Alberta, with only one or two people in a particular postal code, it is easy to identify the person if you have postal code, gender and age. The longitudinal nature of the request (i.e., information for the last 3 years) could also identify the patient, because a meaningless identifier, which stays constant with time, could highlight patient patterns.

C requests R to comply with the requirements for a request for individually identifying information. R is furious because a request for individually identifying information must, in compliance with the Act, be also approved by a Health Research Ethics Board in Alberta. Once approved, R would need to take the Ethics Board's approval and recommendations to C. C would then need to ensure that the recommendations are complied with. Prior to information disclosure, C could then impose additional requirements on R in an information sharing/research agreement. This could include the requirement to complete a Privacy Impact Assessment (PIA) for review and acceptance by the Information and Privacy Commissioner, which could take approximately four to six months to complete. This could jeopardize R's business arrangements and market advantage, which could delay timely research, innovation, and ultimately patient treatment and care.

This confusion has stemmed from broad privacy classification of health information, different interpretations of the term non-identifying information, lack of precise definitions and guidelines, and corresponding privacy protection policies and procedures.

## 3.2 Linkage Between Privacy And Security Classification

'Information Privacy' is achieved when a person or an organization has the ability to control or significantly influence the collection, use and disclosure of their personal information.

'Information Security', as it relates to the definition above, is the preservation of the confidentiality, integrity and availability of this information privacy.

Protecting information privacy is one of the top drivers for information security. As it becomes more challenging to protect data, the interdependence between privacy and security should be enhanced. Privacy and security professionals should work together to develop policies and procedures that address both privacy and security in tandem. Security standards should support the effective application of privacy protection in day-to-day business.

From a classification perspective, one could draw the conclusion that linking the privacy classification with an organization's established security classification and corresponding safeguards, could enhance the information privacy protection and facilitate compliance, by clarifying data access, information handling, storage and destruction practices.

# 4 ANALYSIS OF PRIVACY CLASSIFICATIONS

Privacy classification in the following legislations, guidelines, and best practices, have been reviewed, analyzed, and built upon to determine the proposed privacy classification for health information in Alberta:

- Privacy Classification in Canadian legislation;
- Privacy Classification in Canada's Health Informatics Association Guidelines;
- Privacy Classification in the Government of Alberta Privacy Architecture;
- Privacy Classification in the United States Privacy Legislation.

## 4.1 PRIVACY CLASSIFICATION IN CANADIAN LEGISLATION

The Privacy Commissioner of Canada, in her Fact Sheet – Privacy Legislation in Canada, states that:

- Individuals are protected by the Personal Information Protection and Electronic Documents Act (PIPEDA) that sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities.
- Every province and territory has privacy legislation governing the collection, use and disclosure of personal information held by government agencies.
- Newfoundland and Labrador has passed legislation, but it is not yet in force.
- British Columbia, Alberta and Quebec are the only provinces with laws recognized as substantially similar to PIPEDA. These laws regulate the collection, use and disclosure of personal information by businesses and other organizations.
- Alberta, Saskatchewan, Manitoba and Ontario have passed legislation to deal specifically with the collection, use and disclosure of personal health information by health care providers and other health care organizations.
- Several federal and provincial sector specific laws include provisions dealing with the protection of personal information.

### ANALYSIS

Some Canadian privacy legislations define the term 'personal information' as recorded information about an identifiable individual, while others define 'personal information' or 'individually identifiable information' to mean information about an identifiable individual. Several of these legislations also define personal or individually identifying health information.

It appears that Canadian privacy legislation is very similar to the Alberta health information legislation, with stringent rules around the collection, use and disclosure of personal or individually identifying information, but a lack of clear definitions or rules for any information that does not fall into the personal or individually identifying information classification.

## 4.2 PRIVACY CLASSIFICATION IN THE COACH GUIDELINES

Canada's Health Informatics Association (COACH) Guidelines for Protection of Health Information sets the framework of controls to maximize integrity, minimize risks and protect information in areas of privacy and security. It has often been used as the standard for privacy and security of health information in Canada. It is an additional resource and a companion to the Alberta Health Information Act.

It gives an example of classification of health information in the following three levels:

- Demographic information e.g., name, address, date of birth, gender, identifier numbers.
- Clinical information of a wide variation.
- Highly sensitive clinical or other information, e.g., HIV information, Sexually Transmitted Disease information, mental health information.

### ANALYSIS

The example above is not perfect and cannot be used in every situation. Further, the document states that once information is classified, implementing the classification poses other problems. It is believed that this complexity and difficulty has led to data classification not being adopted at all.

The COACH Guidelines state that the primary concern for classification is context and sensitivity of personal health information to support access levels based on the organization's business requirements. It goes on to mention that classification of information will change over the life of the information, and must be periodically reviewed by someone assigned the responsibility in the organization. The document stresses the need to have a classification scheme as it has a role to play in information access, information handling, storage and destruction practices.

## 4.3 PRIVACY CLASSIFICATION IN THE ALBERTA GOVERNMENT PRIVACY ARCHITECTURE

A popular phrase in privacy circles today is "Privacy by Design". This refers to the need to make privacy protection an integral feature of information technology systems and applications. In 2002, the Government of Alberta, with the assistance of IBM Global Services and the IBM Privacy Research Lab in Zurich, was one of the first organizations to recognize the value of compiling a structured privacy guide connecting its privacy obligations with its existing Government of Alberta Enterprise Architecture (GAEA) for information technology. Extensive research was conducted, including an in-dept review of the existing Alberta privacy legislations as well as industry leading thought on privacy in a technology context. This saw the development of the GAEA Privacy Architecture. This Privacy Architecture represents many new and innovative concepts, techniques and approaches on the road to implementing Privacy by Design.

The GAEA Privacy Architecture comprises of eight Guidance Elements and implementation recommendations. One of the fundamental general requirements of the GAEA Privacy Architecture is that it aligns with, and supports the eight GAEA Privacy Principles. GAEA Privacy Architecture Table 1 shows how these Guidance Elements align with the Privacy Principles.

**Table 1: GAEA Privacy Architecture - Guidance Elements & Privacy Principles**

| **GAEA Privacy Architecture - Privacy Principles** | 1. Collection Limitation | 2. Data Quality | 3. Purpose Specification | 4. Use Limitation | 5. Security Safeguards | 6. Openness | 7. Access | 8. Accountability |
|---|---|---|---|---|---|---|---|---|
| **GAEA Privacy Architecture - Guidance Elements** | | | | | | | | |
| 1. Privacy Glossary | | | X | | | X | | |
| **2. Privacy Taxonomy** | | | | **X** | | | **X** | |
| 3. Identity Key Scheme | | | | X | X | | X | |
| 4. Privacy Design Guidance | X | X | X | X | X | X | | |
| 5. Privacy Transformation | | | | X | | | | |
| 6. Active Privacy Architecture | | | X | X | | | X | X |
| 7. Data Placement | | X | | | | | | |
| 8. Private Access | | | | | | | X | |

The Government of Alberta requirement for data classification resulted in the development of a guidance element called the Privacy Taxonomy, rather than a privacy classification.

Based on recognized industry standards and direction, the GAEA Privacy Architecture defined Privacy Taxonomy addresses the requirements for data classification and also provides a comprehensive scheme to consistently label privacy-related objects and actions in an information technology environment. Privacy Taxonomy for personal information metadata provides the syntax and vocabulary for future rule-based privacy functions to assist with data sharing decisions within the Government of Alberta. The document states that implementation of the Privacy Taxonomy will help to increase speed and strategic alignment of both design and operational decisions in areas such as placement, security, handling and audit of personal information.

The GAEA Privacy Architecture tell us that the Privacy Taxonomy has several dimensions, as illustrated in Figure 1 below, which allow different privacy-relevant attributes to be expressed as required. It has a **Data Dimension**, which expresses attributes that are properties of the personal information itself. It also has a **Policy Dimension**, which expresses attributes that are needed to describe the policies that apply to the data. These policy dimensions are organized into **Intent**, **Conditions** and **Consequences** groupings, which prepare the way for policy to be described in a format that can be interpreted by technology at some future point.

Data dimensions represent characteristics of the data and do not change when policy changes (although a policy change may result in data classification needing to be more granular).

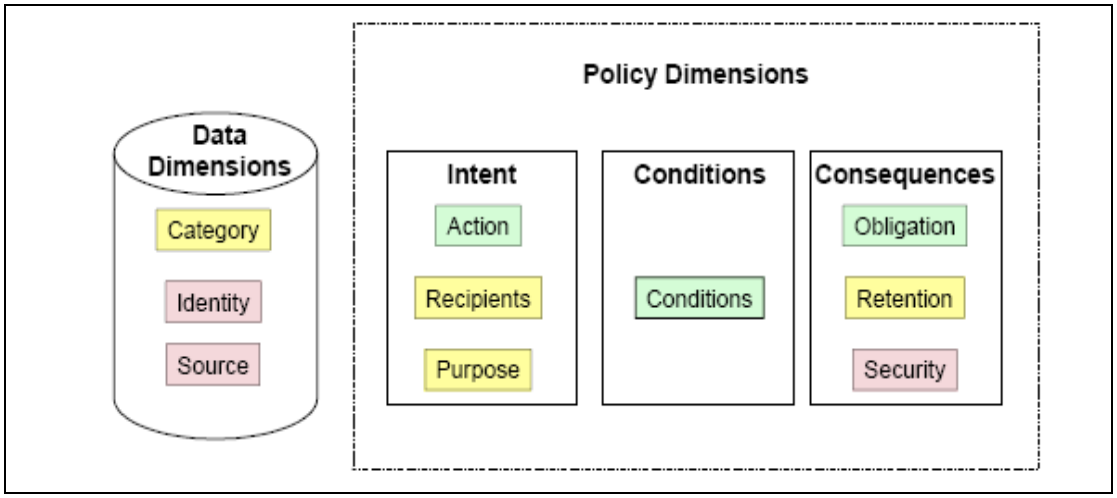



**Figure 1: GAEA Privacy Architecture - Privacy Taxonomy Dimensions**[1]

Of relevance to this research paper is that the Privacy Taxonomy in the GAEA Privacy Architecture also includes a means of describing the identity level of the data in an information technology environment, as shown in Table 2 below.

**Table 2: GAEA Privacy Architecture: Privacy Taxonomy, Data Dimensions - Identity**

| Identity | Meaning |
|---|---|
| Personal Information | Information about an individual that includes information that readily identifies the individual. |
| De-Identified Information | Information about an individual where the identifiers have been removed but keys have been retained to allow identity to be re-attached under the appropriate circumstances |
| Weakly Anonymized Information | Information about an individual where any identifiers have been permanently removed and the remaining information has not been transformed to further mask the identity of the individuals |
| Strongly Anonymized Information | Information about an individual where any identifiers have been permanently removed and the remaining information has been transformed to further mask the identity of the individuals |
| Aggregated Information | Non-identifying information about groups of individuals |

[1] **Data Dimensions:**
- Category, e.g., contact data, health data.
- Identity, e.g., personal information, anonymous information.
- Source, e.g., collected from the individual, derived, opinion.

**Policy Dimensions - Intent:**
- Actions, e.g., collect, modify, use, transform, delete, disclose.
- Purpose, e.g., provide health services, research, law enforcement.
- Recipient, e.g., us or our agents.

**Policy Dimensions – Conditions:**
- Conditions, e.g., require data subject consent, requires proof of authority.

**Policy Dimensions – Consequences:**
- Obligations, e.g., inform data subject of right to appeal decision.
- Retention, e.g., retain for purpose only.
- Security, e.g., security level required to protect the information

Also of relevance to this paper is the Privacy Taxonomy, Security Dimension depicted in the GAEA Privacy Architecture and Table 3 below. This dimension is the existing GAEA security classification. This is classed as a consequence dimension because currently there are no static rules to determine the security level by merely looking at data dimensions like category and identity.

**Table 3: GAEA Privacy Architecture: Privacy Taxonomy, Policy Dimensions - Security**

| Security | Meaning |
|---|---|
| Restricted | Access is specific to an individual and very limited |
| Confidential | Access is specific to a function, group or role |
| Protected | Access is available to those possessing an authenticated identity |
| Unrestricted | Access is unrestricted |

The GAEA Privacy Architecture recommends adoption of the Privacy Taxonomy and promotion of its use in building a 'metadata' description of all databases containing personal information.

Ultimately, adoption of the entire GAEA Privacy Taxonomy with all its dimensions, as a government-wide standard could have the following short term benefits:

- Facilitate separation of data for storage and transformation;
- Provide a basis for identifying data sharing opportunities;
- Facilitate the processing of private access requests;
- Provide consistent input to Privacy Impact Assessments for data sharing and security decisions;
- Provide a basis for auditing proper handling of individually identifying information.

### ANALYSIS

- Most of the GAEA Privacy Architecture concepts can serve as a pro-active checklist either during software design or as part of software acquisition requirements. It can be implemented gradually, as new applications are developing and existing ones are replaced. However, it becomes very difficult, tremendously expensive, and may not be reasonable to incorporate these concepts into technology already in existence.

- This GAEA Privacy Architecture is focused only on information technology for structured, on-line electronic information, and does not fully address the means of adhering to legislated privacy rules in an unstructured, non information technology environment e.g., hard copy information, off-line information, archive tape backup.

**Recommendation:** A classification scheme similar to an information security classification scheme, though typically one dimensional, is simple and could imply a fixed set of consequences that are mandatory to apply. With the establishment of privacy classification integrated with security classification, information protection requirements can be quickly understood, communicated and acted upon. This could facilitate immediate privacy adherence in a non information technology environment, till the data sets are migrated to a more information technology structured electronic environment adhering to the GAEA Privacy Architecture.

- The GAEA Privacy Architecture is required to be followed by all ministries in the Government of Alberta, while the Health Information Act and Regulations are legislated for the entire Alberta publicly funded health sector, and the general public. It becomes difficult to mandate the GAEA Privacy Architecture to this wider audience.

**Recommendation:** As the gap between individually identifying information and non-identifying information is broad and the terms are poorly defined, it would be beneficial to see health information legislation define and clarify a more granular privacy classification scheme. This clarity could facilitate greater understanding and better administration of the legislation. Communication of this legislation could create greater public awareness of privacy protection rules, and as custodians must adhere to privacy protection legislation, this would increase public confidence that their health information is protected.

## 4.4 Privacy Classification In The United States Privacy Legislation

On April 14, 2002 the United States Department of Health and Human Sciences published the Privacy Rule to implement a requirement of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. This Privacy Rule creates national standards to protect electronic transmission of individuals' medical records and other personal health information provided to health plans, doctors, hospitals and other health care providers. The following are the three privacy classifications of information described in the HIPAA and the Privacy Rule:

**Individually Identifying Health Information** is Protected Health Information and includes demographic information that identifies the individual or for which there is a reasonable basis to believe that the information can be used to identify the individual; and relates to:

- the individual's past, present, or future physical or mental health or condition,
- the provision of health care to an individual, or
- the past, present, or future payment for the provision of health care to an individual.

**Limited Data Set** is also Protected Health Information from which specified direct identifiers of individuals, their relatives, household members, and employers have been removed. A limited data set may be used and disclosed for research, health care operations and public health purposes, provided that the recipient has entered into a data use agreement promising specified safeguards for the protected health information with the limited data set.

**Note :** (Source: http://privacy.med.miami.edu/glossary/xd_limited_data_set.htm)
A Limited Data Set must have all direct identifiers removed, including:

- name and social security number;
- street address, e-mail address, telephone and fax numbers;
- certificate/license numbers;
- vehicle identifiers and serial numbers;
- URLs and IP addresses;
- full face photos and any other comparable images;
- medical record numbers, health plan beneficiary numbers, and other account numbers;
- device identifiers and serial numbers; and
- biometric identifiers, including finger and voice prints.

A limited data set could include the following **(potentially identifying)** information:

- admission, discharge, and service dates;
- dates of birth and, if applicable, death;
- age 90 or over; and
- full zip code or any other geographic subdivision, such as state, county, city, precinct and their equivalent geocodes (except street address).

**De-Identified Health Information** neither identifies nor provides reasonable basis to identify an individual. There are no restrictions on the use or disclosure of de-identified information. De-identification can be done either:

- as a formal determination by a qualified statistician, or
- by removing identifiers of the individual, their relatives, household members, and employers, such that the remaining information could not be used to identify the individual.

### ANALYSIS

In addition to individually identifying health information and de-identified health information, which is similar to the Health Information Act's individually identifying information and non-identifying information respectively, HIPAA's Privacy Rule makes provisions for a "limited data set". It clearly articulates the identifiers that need to be excluded and the "potential identifiers" that could be included, with appropriate protection. The Health Information Act lacks this level of detail, which could be extremely useful to facilitate understanding, better administration, and ensure compliance with the legislation. I therefore recommend using the limited data set rules in my proposed research solution.

## 5 ANALYSIS OF SECURITY CLASSIFICATION

Our analysis shows that the security classification uses a risk assessment approach based on determining the impact of a loss to integrity, availability or confidentiality of the information.

The Information Security Classification, February 2005 (Government of Alberta Information Management) compares Alberta's information security classification with standards developed in Ontario and the guidelines developed by the Public Sector Chief Information Officers' Council (PSCIC), and the Office of Management and Budget in the United States. It also compares the Government of Alberta information security classification with that of the PSCIC and the Government of Canada.

Much work has been done to ensure that the Alberta Government information security classification as shown in Table 4 below, meets acceptable security standards and is consistent with security classification standards for information assets in other jurisdictions. The security classification uses a risk assessment approach based on determining the impact of a loss to integrity, availability or confidentiality of the information.

## Table 4: Government of Alberta Information Security Classification Guidelines

| Classification | Description | Examples of Information Assets | Examples of Risk Impacts |
|---|---|---|---|
| **Restricted** | Information that is extremely sensitive and could cause **extreme** damage to the integrity, image or effective service delivery of the GoA. Extreme damage includes loss of life, risks to public safety, substantial financial loss, social hardship, and major economic impact. **Restricted information is available only to named individuals or specified positions.** | • Cabinet documents<br>• Cabinet deliberations and supporting documents<br>• Personal medical records<br>• Provincial budget prior to public release<br>• Criminal investigation | • Loss of life<br>• Extreme or serious injury<br>• Loss of public safety<br>• Significant financial loss<br>• Compromise of the legal system<br>• Compromise of Cabinet deliberations<br>• Destruction of partnerships and relationships<br>• Significant damage<br>• Sabotage/terrorism<br>• Extreme risk if corrupted or modified |
| **Confidential** | Information that is sensitive within the GoA and could cause **serious** loss of privacy, competitive advantage, loss of confidence in government programs, damage to partnerships, relationships and reputation. It includes highly sensitive personal information. **Confidential information is available only to a specific function, group or role.** | • Personal case files such as benefits, program files or personnel files<br>• Industrial trade secrets<br>• Registration information<br>• Personnel files<br>• Policy advice<br>• 3rd party business information submitted in confidence | • loss of reputation or competitive advantage<br>• loss of confidence in the government program<br>• loss of personal or individual privacy<br>• loss of trade secrets or intellectual property<br>• loss of opportunity (e.g., health coverage)<br>• financial loss<br>• high degree of risk if corrupted or modified |
| **Protected** | Information that is sensitive outside the Government of Alberta (GoA) and could impact service levels or performance, or result in low levels of financial loss to individuals or enterprises. Protected information would include personal information, financial information or details concerning the effective operation of the GoA, ministries and departments. **Protected information is available to employees and authorized non-employees (contractors, sub-contractors and agents) possessing a need to know for business-related purposes.** | • Policy interpretation<br>• Draft request for proposals<br>• Business information<br>• Applications<br>• Planning documents<br>• Documents containing personal information | • Unfair competitive advantage<br>• Disruption to business if not available<br>• Low degree of risk if corrupted or modified |
| **Unrestricted** | Information that is created in the normal course of business that is unlikely to cause harm. It includes information deemed public by legislation or through a policy of routine disclosure and active dissemination. **Unrestricted information is available to the public, employees and contractors, sub-contractors and agents working for the government.** | • Public health information<br>• Job postings<br>• Ordinary staff meeting agendas and minutes<br>• Research and background papers (with no copyright restrictions) | • Little or no impact<br>• Minimal inconvenience if not available<br>• If lost, changed or denied would not result in injury to an individual or government (that is, no legal effect) |

# 6 PROPOSED SOLUTION

As we have seen, protecting information privacy is one of the top drivers for information security. Accordingly, security standards should support the effective application of privacy protection in day-to-day business. From a classification perspective linking the privacy classification with an organization's established security classification and corresponding safeguards, could enhance the information privacy protection and facilitate compliance, by clarifying data access, information handling, storage and destruction practices.

Accordingly, my proposed solution to privacy classification issues comprises of three parts:

- A simple and effective privacy classification guideline for health information in Alberta, linking with corresponding security requirements and safeguards, to enhance overall privacy protection. This could imply a fixed set of consequences that are mandatory to apply.
- An Alberta Health Information Regulation including clarifying definitions to assist with privacy classification. This could make privacy protection requirements easy to understand, to communicate, and to act upon.
- Preliminary guidance on implementing the privacy classification guidelines, facilitating health information assessment and protection.

## 6.1 PRIVACY CLASSIFICATION GUIDELINE FOR HEALTH INFORMATION IN ALBERTA

The proposed privacy classification in Table 5 below builds on pieces of work completed and analysed in the earlier sections of this paper. As you see, the privacy classification has been aligned with the Government of Alberta Information Security Classification, with appropriate safeguards listed for each category.

This privacy classification should be used within the privacy framework of the organization, in combination with privacy legislation, relevant policies/standards, and privacy procedures for collection, use and disclosure of health information. The privacy classification could facilitate immediate privacy adherence in a non information technology environment, till the data sets are migrated to an information technology structured electronic environment built to adhere to the guidance elements in the GAEA Privacy Architecture.

## Table 5: Proposed Privacy Classification Guideline for Health Information in Alberta

| # | Security Level | Privacy Classification | Safeguards | | | |
|---|---|---|---|---|---|---|
| | | | **Storage & Transmission** | **Access** | **Disposal** | **Privacy Legislation** |
| A. | **Restricted** | **Individually Identifying Information** that is highly sensitive, i.e., improper collection, use or disclosure of this information could damage the integrity, image or operation of the organization.<br><br>**Examples of 'Restricted' Individually Identifying Information:**<br>• Information requiring specific consent for access.<br>• Highly sensitive clinical or other data, e.g., HIV data, Sexually Transmitted Disease data, mental health data.<br>• Information that the individual requests to be electronically masked, or treated as highly sensitive, e.g., abortion data, mental health data. | • Stored in highly secure zone, with access tracking and audit trail for all access points (e.g., signatures).<br>• Data encrypted, password protected, double authenticated, audited and monitored.<br>• Courier transport supervised by staff.<br>• Tamper evident packaging.<br>• Clean desk policy. | • Access is specific and very limited to named individuals or role with the required consent.<br>• All access or actions are logged and subject to non-repudiation processes, as appropriate. | • Shred or destroy data or media with certificate of destruction. | • Collect, use, or disclose in accordance with the Health Information Act.<br>• Privacy Impact Assessment and/or Ethics Review, as required.<br>• Security Assessment, as required.<br>• Information sharing agreements, as required, specifying among other things:<br>o Data use/disclosure.<br>o Protection of confidentiality, integrity and availability of data and immediate reporting on any breach of same.<br>o Agents and subcontractors to adhere to the terms of the agreement. |
| B. | **Confidential** | **Individually identifying information**, i.e., where the identity of the individual who is the subject of the information can be *readily ascertained*.<br><br>**Potentially identifying information,** i.e., information about an individual *where identifiers have been removed*, but the identity of the individual can be *ascertained under certain circumstances*.<br><br>**Examples of Potentially Identifying Information:**<br>• Longitudinal data, i.e., information without unique identifiers, at an individual level, with data for a long period, e.g., more than 1 year.<br>• HIPAA defined Limited Data Set with potentially identifying information, as shown in section 4.4 of this paper.<br>• Information with a small data cell, e.g., 5 or less elements in the data set.<br>• De-Identified Information; and Weakly Anonymized Information; as defined in the GAEA Privacy Architecture and section 4.3, Table 2 of this paper. | • Secure location with restricted access.<br>• Clean desk policy.<br>• Encrypted, secure transmission, e.g. Secure File Transfer Protocol.<br>• If encrypted, secure transmission is not possible, a sealed envelope, secure courier, marked 'to be open by addressee only'.<br>• Receipt confirmation required. | • Access is specific to a function, group or role.<br>• Authorized access and authenticated access required to protect information from unauthorized disclosure or modification.<br>• Log access/ actions.<br>• Periodic audits of adequate protection. | • Shred/ destroy data or media with certificate of destruction. | • Collect, use, or disclose in accordance with the Health Information Act.<br>• Privacy Impact Assessment and/or Ethics Review, as required.<br>• Security Assessment, as required.<br>• Information sharing agreements, as required, specifying among other things:<br>o Data use/disclosure.<br>o Protection of confidentiality, integrity and availability of data and immediate reporting on any breach of same.<br>o Agents and subcontractors to adhere to the terms of the agreement.<br>o If data is potentially identifying, no re-identification of individuals who are the subject of the data. |

| # | Security Level | Privacy Classification | Safeguards | | | |
|---|---|---|---|---|---|---|
| | | | **Storage & Transmission** | **Access** | **Disposal** | **Privacy Legislation** |
| C. | **Protected** | **Non-identifiable information**, i.e., where the identity of the individual who is the subject of the information cannot be readily ascertained.<br><br>**Examples of non-identifying information:**<br>• HIPAA defined Limited Data Set without the potentially identifying data sets as shown in section 4.4 of this paper.<br>• Information without unique identifiers, at an individual level, with data for a short period time, e.g., less than 1 year.<br>• Strongly Anonymized Information, as defined in the GAEA Privacy Architecture and section 4.3, Table 2 of this paper. | • Sealed envelope.<br>• Secure courier.<br>• Password protect, as necessary.<br>• Secure location. | • Access is available to those possessing an authenticated identity.<br>• Group authorized access on a need-to-know basis for business related purposes. | Shred/delete and empty 'recycle bin' folder. | • Collect, use, or disclose in accordance with the Health Information Act.<br>• Complete the Health Information Act section 32(2) Data Disclosure Form.<br>• If information is disclosed to a non-custodian, the non-custodian must be advised to notify the Alberta Information Privacy Commissioner if they wish to use the information for data-matching. |
| D. | Unrestricted | **Aggregate information**, i.e., non-identifying information about groups of individuals.<br><br>**Examples of aggregate information:**<br>• Information available to the public.<br>• Cohort level information, e.g., age group 0-10. | • Controls in place to protect the integrity of the data and prevent unauthorized modification. | • Access is unrestricted. | • No specific security requirements. | • No specific security requirements. |

## 6.2 AMENDING THE HEALTH INFORMATION REGULATION

While the existing health information legislation defines individually identifying information, non-identifying information and aggregate information, there is no detail around what is exactly meant by each term. In addition, the range between individually identifying information and non-identifying information appears to be large. Non-identifying information means different things to different people, causing much confusion while administering the legislation. This warrants another privacy classification of health information, i.e., **potentially identifying information,** to narrow the scope, and focus the classification and appropriate safeguards for access, storage, transmission, and data destruction of the information.

**It is proposed that the Health Information Regulation define the new term "potentially identifying information" to mean information about an individual where identifiers have been removed, but the identity of the individual can be ascertained under certain circumstances.**

The privacy classification guidelines for health information in Alberta, with newly defined terms and a more detailed and clarifying explanation of existing terms, warrants communication of these definitions and examples to the Alberta health sector and the general public.

The health information regulation appears to be the most appropriate vehicle to communicate the privacy enhancement to this wide audience. Incorporating privacy protection in the legislation also mandates Alberta health sector compliance, and ensures the Albertan that their health information is protected.

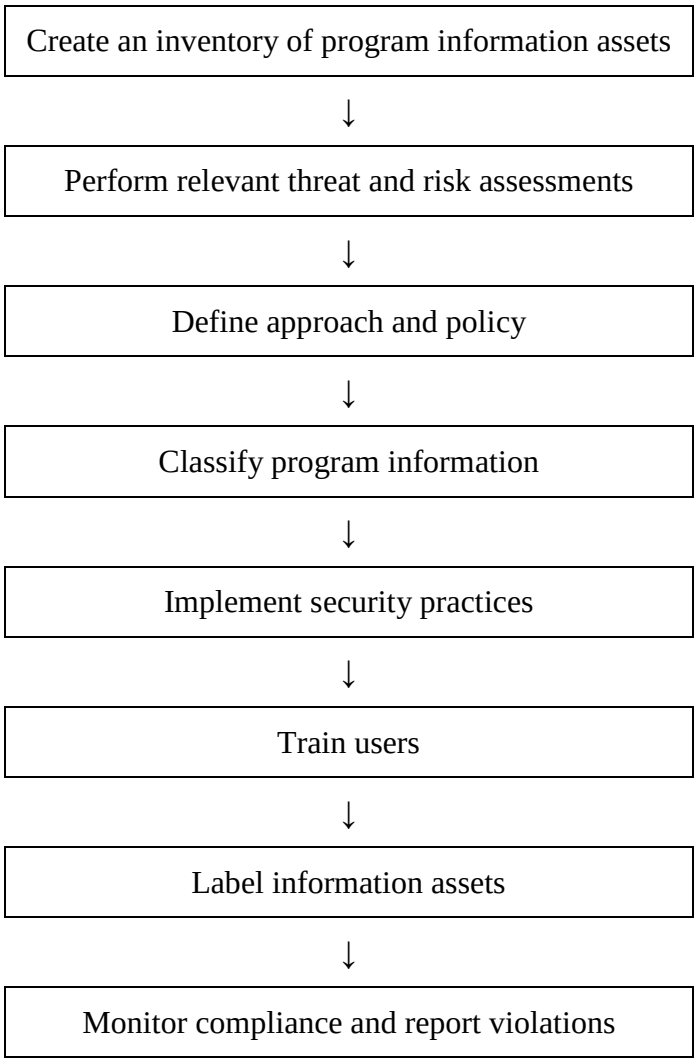
It is also proposed that the Health Information Act Guidelines and Practices Manual include the Privacy Classification Guideline for Health Information in Alberta, and provide examples of individually identifying information, potentially identifying information, non-identifying information, and aggregate information. This could add clarity to definitions that are currently ambiguous. The legislation could then become easier to understand, to administer, to monitor and to audit. This could enhance privacy protection of health information, and the average Albertan could trust that their health information is protected.

## 6.3 IMPLEMENTING THE PRIVACY CLASSIFICATION GUIDELINE

The privacy classification guideline, with an amending health information regulation, could facilitate immediate privacy adherence in the Alberta health sector. This could also facilitate health sector awareness and possibly gradual acceptance of something similar to the GAEA Privacy Architecture, as new applications develop, existing ones are replaced, and all data sets are migrated to a more information technology structured environment.

As the privacy classification guideline is linked with the security classification guideline, the process for implementing the privacy classification guideline could be the same as the process developed for implementing information security classification, as stated in Information Security Classification (Government of Alberta – February 2005), and highlighted as follows:

**Table 6: Implementing the Privacy Classification Guideline**
(Source: Information Security Classification, Government of Alberta)




Preliminary guidance on implementing the privacy classification guideline includes:

- Use the privacy classification guideline within the privacy framework of the organization, in combination with privacy legislation, relevant policies/standards, and organizational privacy procedures for collection, use and disclosure of health information.

- The privacy classification guideline should be used in combination with other organizational policies and procedures e.g., human resources, information management, information technology, information security, finance.

- The Chief Information Officer of the organization should be responsible for overseeing the privacy and security compliance with legislation, policies and procedures.

- Information owners or the originating program area should be designated to assign and label the information classification to the information holdings that they manage, and ensure that all information is appropriately classified and protected according to their classification level. The information owners should adhere to the safeguards assigned to the classification of the organization's information collected, used or disclosed.

- The duration of the classification ratings, declassification dates, triggers, or other pertinent information may also need to be addressed and documented while labelling all information assets appropriately with their classification ratings.

- The classification of information may change with time, under certain circumstances, or with new technological developments, so it is important that information owners periodically, e.g., once every 3 years, review the classification assigned.

- Program managers should be responsible for ensuring that anyone who collects, uses or discloses information is appropriately trained to understand the type of health information, its corresponding sensitivity and safeguards. Users should be trained in the requirements of relevant Alberta privacy legislations. Users should also be trained to meet the requirements for labelling, storing, transmitting information, and access control, to protect against unauthorized access to the information.

- Procedures for ongoing monitoring of compliance, and reporting of violations and breaches to privacy protection should be established and adhered to.

Successful implementation of the privacy protection will allow custodians and their affiliates to perform their duties effectively, while preserving public trust that their health information is protected.

# 7 BENEFITS OF PROPOSED SOLUTION

The privacy classification guideline for health information in Alberta, and an amendment to the health information regulation to clarify privacy definitions, will have the following positive impact on privacy protection.

### FOR THE HEALTH INFORMATION CUSTODIAN/AFFILIATE

- Facilitates greater understanding of the different categories and appropriate management and protection of health information.
- Enables clear and effective communication of privacy classification and corresponding privacy protection to the Alberta health sector.
- Helps with better administration of the legislation, policies and procedures and improved ability to audit compliance with the privacy protection processes.
- Facilitates the processing of requests for access to information, and the protection against unauthorized access to health information.
- Minimizes the risk of re-identification of data by applying appropriate safeguards.
- Provides the basis for identifying data sharing opportunities, and assists with data sharing decisions.

- Facilitates consistent input to Privacy Impact Assessments for the collection, use and disclosure of health information.

### FOR THE HEALTH INFORMATION USER

- Enables greater understanding of health information categories, appropriate safeguards, access levels and information protection practices, and thereby enhances privacy protection.

### FOR THE REQUESTOR OF INFORMATION

- Creates awareness of protection processes and timelines required for release of the various categories of health information. This creates the ability to plan effectively for data requests.

### FOR THE ALBERTA HEALTH SECTOR

- Provides clear and better defined privacy legislation and privacy classification guidelines.
- Facilitates greater understanding and compliance with well defined privacy protection processes and safeguards.

### FOR ALBERTANS

- Creates awareness of legislated processes to protect the privacy and confidentiality of an individual's health information.
- As health information protection is mandated, provides greater confidence and trust that an Albertan's information is protected.

## 8 DISCUSSION

This provides an additional explanation of the results achieved, and highlights the following:

- **Reference to Previous Work:** It must be reiterated that the Privacy Classification Guideline for Health Information in Alberta builds on, and links existing best practices of privacy and security work conducted in Alberta, Canada, and the United States of America.

- **New Privacy Classification Category:** The gap between individually identifying information and non-identifying information is broad and the terms are poorly defined. It is recommended that a new privacy classification, i.e., 'potentially identifiable information' be defined in the Health Information Regulation. This more granular privacy classification category will take the guesswork out of determining whether the information without unique identifiers is non-identifying or individually identifying. It will facilitate understanding and better administration of the legislation.

- **Regulatory Reform:** The Health Information Act does not prevent custodians from agreeing on a common privacy classification guideline. However, having the entire Alberta health sector agree on a new definition can be rather challenging. To alleviate this issue, mandating compliance with the defined classification 'potentially identifying information' through the Health Information Regulation is my preferred solution. The Privacy Classification Guidelines with examples, and guidance on implementing the Privacy Classification Guidelnes could then be detailed in a companion document.

- **Companion Document:** The proposed solution also recommends that the Health Information Act Guidelines and Practices Manual include the Privacy Classification Guidelines for Health Information in Alberta. It should include concrete examples of the terms 'individually identifiable information', 'potentially identifiable information', 'non-identifiable information' and 'aggregate information'. It is further recommended that the guidelines for implementing the Privacy Classification Guidelines also be included in the Health Information Act Practices Manual. With this additional information, the Health Information Act Guidelines and Practices Manual could serve as an enhanced resource and companion document to users and administrators of Alberta health information legislation.

- **Subjective:** While the Privacy Classification Guideline for Health Information in Alberta is written to provide clarity and detail, it is written in a subjective manner to cover the scope of complex privacy issues experienced in the Alberta health sector. It guides the reader to categorize the information into privacy classifications by providing examples rather than categorical statements. This permits some flexibility and subjectivity based on a case-by-case analysis. One such example is "Information with a small data cell, e.g., 5 or less elements".

- **Wider Scope:** Privacy legislation across Canada is quite similar, and written with the focus on personal information or individually identifying information. These Privacy Classification Guidelines, with the added category of potentially identifying information, and clarifying examples, could serve as a useful tool not only for health information in Alberta, but also for health information in other provinces in Canada.

# 9 CONCLUSION

Recipients of health information, internal and external to the organization, may be unaware of the value or sensitivity of the information requested. Privacy classification of health information and corresponding privacy legislation is essential for information protection to be quickly understood, communicated and acted upon.

The proposed privacy classification guideline, linked to the existing information security classification guideline, will complement and enhance Alberta's existing health information privacy protection processes. This more granular privacy classification will assist Alberta's entire health sector with clear categories of data, reduce the risk of re-identification of data, and increase privacy protection rules that are effective, efficient, and easier to understand and administer.

Albertans need to understand the rules for protection of their health information and they need to trust that their health information is protected.

# 10 REFERENCES

## Documents


COACH Guidelines for the Protection of Health Information – December 15, 2007
©COACH: Canada's Health Informatics Association

GAEA (Government of Alberta Enterprise Architecture) Privacy Architecture – Privacy Glossary. http://www.sharp.gov.ab.ca/docDisplay.cfm?DocID=4403&nh=1

GAEA (Government of Alberta Enterprise Architecture) Privacy Architecture
http://www.sharp.gov.ab.ca/docDisplay.cfm?DocID=4401&nh=1

Health Information Act Guidelines and Practices Manual (HIA02 2007)
http://www.health.gov.ab.ca/about/HIA_Guidelines-Practices-Manual.pdf

Information Security Classification, February 2005 (Information Management - Government of Alberta). http://www.im.gov.ab.ca/publications/pdf/InfoSecurityClassification.pdf

Lucock, C. (2005). Guidelines Workshop: Anonymization of Electronic Health Information Data. http://idtrail.org/files/Handout_final.pdf

Limited Data Set (Health Insurance Portability and Accountability Act [HIPAA])
Privacy/Data Protection Project – University of Miami
http://privacy.med.miami.edu/glossary/xd_limited_data_set.htm

Privacy Legislation In Canada - Fact Sheet
http://www.privcom.gc.ca/fsfi/02_05_d_15_e.asp

Summary of the HIPPA Privacy Rule – HIPPA Compliance Assistance – United States Department of Health and Human Services. http://www.hhs.gov/ocr/privacysummary.pdf


## Legislation


*Health Information Act* 2001 (Alberta).
http://www.qp.gov.ab.ca/documents/Acts/H05.cfm?frm_isbn=0779719352&type=htm

*Health Insurance Portability and Accountability Act* 1996 (USA)
http://www.hhs.gov/ocr/privacysummary.pdf

Provincial / Territorial Privacy Laws, Oversight Offices and Government Organizations
http://www.privcom.gc.ca/resource/prov/index_e.asp