

Agenda: Privacy Legislation in Alberta *Implications to Supporting Dental Industry*



- Registration Desk (8:45 AM)
 - Welcome and Introductions (9:00 AM)
 - Why we are here and agenda
 - Privacy 101:
 - Background on privacy legislation in Alberta
 - Definition of health information
 - Custodians and affiliates
 - Implications of being classed as an affiliate
 - Responsibilities
 - Moving forward together to meet our collective obligations under the Health Information Act
 - Key sections and concepts from the Health Information Act
 - Confidentiality oaths, contractor agreements and information manager agreements
 - Information Security and Privacy policies
 - Case scenarios
 - Electronic Health Record System requirements
 - Case scenarios
 - Privacy Impact Assessment requirements
 - Case scenarios
 - Alberta Netcare and the future
 - Alberta Dental Association and College initiatives
 - Open session: Questions and Answers; What is next? What are the issues? Other topics?
 - Wrap up and thank you (12 noon)
-
- ❖ Break for coffee and refreshments around 10:15
 - ❖ Plan is to be finished by 12 noon
 - ❖ Afternoon is available and can be structured in a variety of ways such as one on one sessions, group discussion or specific topics depending on needs of participants

Privacy Legislation in Alberta

Implications to Supporting Dental Industry

Hosted by the Alberta Dental Association and College

April 3, 2017, 9 AM to 12 Noon (afternoon if required)

Varscona Hotel, Edmonton Alberta



Welcome to everyone from the Alberta Dental Association and College



Special thank you to *Alberta Health* and *the Office of the Information and Privacy Commissioner* who have been working with the *Alberta Dental Association and College* on what could be described as a “new adventure”.

With us today are:

Nji Lionel Nji, *Senior Information Privacy and Security Manager, Office of the Information and Privacy Commissioner* (Dental Profession Portfolio Lead)

Silvia Russell, *Provincial E-Health Policy Advisor, Health Information Act Policy, Privacy and Security Unit, Alberta Health* (New Authorized Custodian Implementation Project Lead)

Brian Hamilton, *eHealth Support Services Lead, Privacy and Security*

Who are we?

- Dentists
- Work in the area of membership support with the Alberta Dental Association and College
- Current focus is legislated requirements of the Health Information Act and how to assist dentists with meeting their obligations
- Integration of dentists into Alberta Netcare

Harry Ames, BA, DDS

- Membership Services Coordinator Alberta Dental Association and College
- 20 years rural/urban private practice New Brunswick
- 10 years various roles Health Canada
- Ottawa Clinic for the underprivileged
- Mediation committee New Brunswick Dental Society



Darryl Smith, BSc DDS

- 35 years in a rural general practice in Northern Alberta
- Past President Alberta Dental Association
- Past President Canadian Dental Association
- Dental Advisor Alberta Dental Association and College
- Fellow PFA, ICD and ACD



Want to provide some background on why we are here today and short agenda

- Intention is to transfer knowledge, answer questions, problem solve, seek solutions and be interactive
- At the end of the day know what are our collective obligations and responsibilities
- Understanding of where health care is heading and how this will change dental practices, the profession and the supporting dental industry
- Need you to spread the message to others

Privacy 101 – Everyone in this room falls under legislated privacy obligations and responsibilities whether we realize it or not

- Privacy Act Canada 1985
- Freedom of Information and Protection of Privacy Act Alberta 1995 (FOIP)
- Personal Information and Electronic Document Act Canada 2000 (PIPEDA)
- Personal Information and Privacy Act Alberta 2004 (PIPA)
- Health Information Act Alberta 2001/2011 (HIA)
- Canada's Anti-Spam Legislation 2014 (CASL)
- Digital Privacy Act Canada 2015 (amendments to PIPEDA)



Privacy is not a new concept to Health Professionals



Secrecy and delicacy, when required by peculiar circumstance, should be strictly observed, and the familiar and confidential intercourse to which physicians are admitted in their professional visits, should be used with discretion, and with the most scrupulous regard to fidelity and honour. The obligation to secrecy extends beyond the period of professional services; no circumstance connected with the privacies of personal or domestic life, infirmities of disposition, or stain of character, observed during professional attendance, should ever be divulged by the physician, except when he is imperatively required to do so. So great is the necessity of this obligation that Courts of Justice protect professional men in their observance of secrecy under certain circumstances.

Canadian Medical Association Code of Ethics 1868

Regardless of jurisdiction, privacy legislation is based on common principles

FAIR INFORMATION PRINCIPLES

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure and Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

On the surface differences, but

While it may appear Alberta has taken a different approach, other jurisdictions are moving in the same direction!

Among the changes made by the *Digital Privacy Act* is the establishment of mandatory data breach reporting requirements. These obligations are set out in Division 1.1 of the *Digital Privacy Act*. In summary, organizations that experience a data breach – referred to in the Act as “a breach of security safeguards” – must:

- determine if the breach poses a “real risk of significant harm” to any individual whose personal information was involved in the breach;
- notify individuals as soon as feasible of any breach that poses a “real risk of significant harm”;
- report any data breach that poses a “real risk of significant harm” to the Privacy Commissioner, as soon as feasible;
- where appropriate, notify any third party that the organization experiencing the breach believes is in a position to mitigate the risk of harm; and
- maintain a record of the data breach and make these records available to the Privacy Commissioner upon request.

Data Breach Notification and Reporting Regulations

The Government has the authority to make regulations to provide greater clarity and specificity with respect to the Act’s data breach reporting requirements. This includes the authority to set out the form and content of notifications and reports, additional factors to be considered in the determination of risk and details on record keeping requirements, as well as other elements.

What is a “Breach of Security Safeguards”?

The new data breach reporting requirements in PIPEDA apply to any “breach of security safeguards”. As a result, a clear understanding of this term is required.

Subsection 2(1) of PIPEDA defines a “breach of security safeguards” as:

the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization’s security safeguards that are referred to in Clause 4.7 of Schedule 1 or from a failure to establish those safeguards

The definition is intended to include two elements – the first being that personal information is lost, or accessed by an unauthorized individual (either through theft or wrongful disclosure), and second, that the loss or unauthorized access is the result of someone violating the organization’s security safeguards (or is the result of the organization failing to establish such safeguards).

For example, the failure of an employee to password-protect a database containing customer personal information as required by an organization’s security policy, which resulted in the database being accessed by contract employees not authorized to view it, would meet the definition of a data breach under PIPEDA. However, a failure to password-protect the database alone, without the data being accessed by an unauthorized individual, would not meet the definition of a “breach of security safeguards” in the Act.

PRIVACY IMPACT ASSESSMENT TOOL

CONTENTS

Introduction	1
Frequently Asked Questions	2
Before Getting Started	3
Privacy Impact Assessment Tool	4
Part 1: Summary of Program or Activity	4
Part 2: Describe the Scope	4
Part 3: Collection, Use and Disclosure of Personal (Health) Information	5
Part 4: Access Rights for Individuals	6
Part 5: Privacy and Security Measures	6
Part 6: PIA Summary and Findings	8
Appendices	9

September 2015

Manitoba Ombudsman
725 - 500 Portage Avenue
Winnipeg, MB R3C 3J1

204-982-9130 (phone)
1-800-665-0531 (toll free in Manitoba)
204-942-7863 (fax)
ombudsman@ombudsman.mb.ca
(general email inquiries)

www.ombudsman.mb.ca

Introduction

Under *The Freedom of Information and Protection of Privacy Act* (FIPPA) and *The Personal Health Information Act* (PHIA), public bodies and trustees (organizations) have specific privacy obligations. These include how you collect, use and disclose the public’s personal and personal health information.

Protecting privacy is more than just upholding the law, it also involves taking a proactive approach to safeguarding the public’s personal (health) information.

Risks to privacy can arise in many circumstances. Collecting excessive information, using intrusive means of collection, or obtaining sensitive details in unexpected circumstances all represent risks to the individual. The use or disclosure of that information, or its retention for an unduly long period, puts privacy at risk.

Many organizations use privacy impact assessment (PIA) tools to assist in safeguarding Manitobans’ personal (health) information.

To support organizations in achieving this goal, Manitoba Ombudsman has developed a PIA tool that “tells the story” of a project from a privacy perspective. Simply, it encourages organizations to think about privacy when evaluating an existing or proposed program, service or activity.

It is our intent that this PIA tool will assist organizations in identifying potential privacy risks and as a result, they will be in a better position to address those risks early on.

This PIA tool is not intended to replace any processes you may already have or be a substitute for complying with FIPPA and PHIA. Our office encourages you to review the information gathered through this process with an access and privacy representative (access and privacy coordinator, privacy officer, lawyer, etc.) so that you can address specific privacy requirements.

Acknowledgments

We gratefully acknowledge the contributions of the Nova Scotia department of Justice, British Columbia Office of the Chief Information Officer, University of Manitoba, Office of the Information and Privacy Commissioner of Alberta and New Zealand’s Privacy Commissioner’s Office to our *Privacy Impact Assessment Tool*. Our tool incorporates much of their collective advice and knowledge.

Manitoba Ombudsman

www.ombudsman.mb.ca | ombudsman@ombudsman.mb.ca | 1-800-665-0531 | 204-982-9130

Dentists, like many other health professions in Alberta are legislated under four provincial Acts

Government Organization Act 2000

(What we can do - 2001)

Health Professions Act 2001

(Who we are and how we are governed - 2001)

Personal Information and Privacy Act 2003

(How we conduct our business relationships – 2003)

Health Information Act 2001/2011

(How we communicate to provide health care services - 2011)



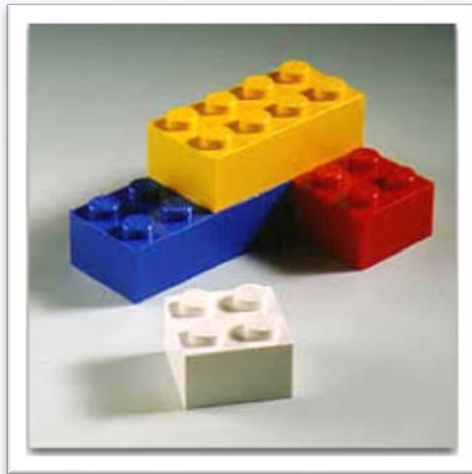
**Health Information Act
will be our focus today**

Need to think of the Health Information Act in broader terms than just privacy.



The Health Information Act is enabling legislation that facilitates the provision of health care by establishing rules and conditions regarding the collection, use and disclosure of health information in an increasingly digital age.

Cornerstones of the Health Information Act



“Need to Know”: must collect, use, disclose only what is needed for the intended purposes,

“Highest Degree of Anonymity”: must collect, use, disclose health info in the most anonymous format or way possible, and

“Least Amount of Info”: must collect, use, disclose only the amount of health info required for the intended purpose.

Need to understand what constitutes health information

The Health Information Act
Section 1 (1) K defines health
information as:

*“health information” means one
or both of the following:*

- (i) diagnostic, treatment and care
information;*
- (ii) registration information*

The image shows a stack of dental forms. The top form is a 'REGISTRATION' form with sections for 'SECTION A: This Patient', 'SECTION B: Acknowledgement of Receipt of Privacy Practices Notice', and 'SECTION C: Good Faith Effort to Obtain Acknowledgement of Receipt'. Below this is a 'CHILD DENTAL MEDICAL HISTORY' form. Underneath that is a 'CHILDREN'S RECALL EXAMINATION' form, followed by a 'CHILDREN'S CLINICAL EXAMINATION' form, a 'TREATMENT PLAN' form, a 'PROBLEM / PRIORITY LIST' form, and finally a 'PROGRESS NOTES' form. The forms are stacked and slightly offset, showing multiple layers.

*diagnostic, treatment
and care information;*



Health Information Act Section 1

(i) “diagnostic, treatment and care information” means information about any of the following:

(i) the physical and mental health of an individual;

(ii) a health service provided to an individual, including the following information respecting a health services provider who provides a health service to that individual:

(A) name;

(B) business title;

(C) business mailing address and business electronic address;

(D) business telephone number and business facsimile number;

(E) type of health services provider;

(F) licence number or any other number assigned to the health services provider by a health professional body to identify that health services provider;

(G) profession;

(H) job classification;

(I) employer;

(J) municipality in which the health services provider’s practice is located;

(K) provincial service provider identification number that is assigned to the health services provider by the Minister to identify the health services provider;

(L) any other information specified in the regulations;

(iii) the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance;

(iv) a drug as defined in the Pharmacy and Drug Act provided to an individual;

(v) a health care aid, device, product, equipment or other item provided to an individual pursuant to a prescription or other authorization;

(vi) the amount of any benefit paid or payable under the Alberta Health Care Insurance Act or any other amount paid or payable in respect of a health service provided to an individual,

and includes any other information about an individual that is collected when a health service is provided to the individual, but does not include information that is not written, photographed, recorded or stored in some manner in a record;

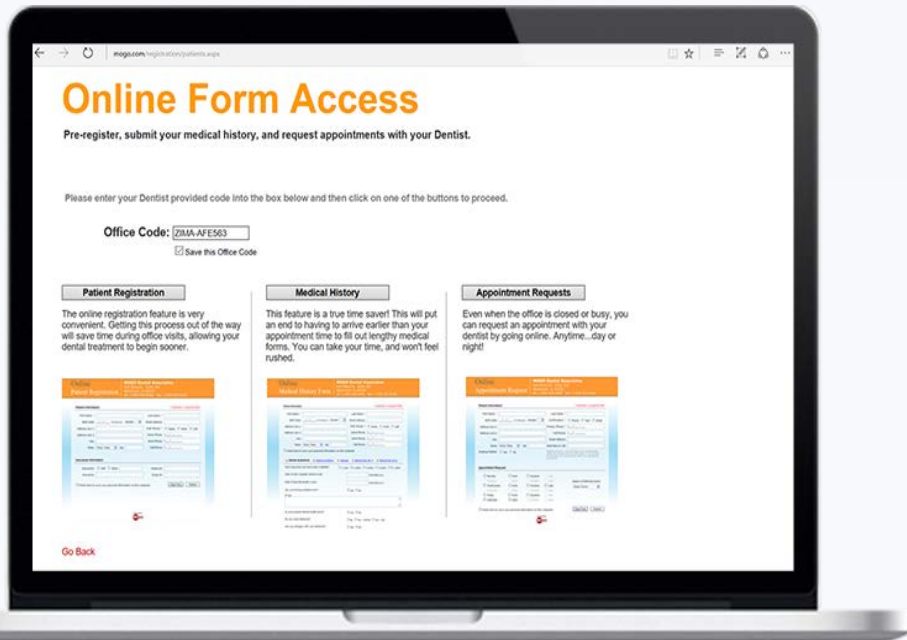
registration information

Registration Information is defined in the Health Information Act
(Section 1 (u) of the Health Information Act and Section 3 of the
Health Information Act Health Information Regulation)

“registration information” means information relating to an individual that falls within the following general categories and is more specifically described in the regulations:

- (i) demographic information, including the individual’s personal health number;
- (ii) location information;
- (iii) telecommunications information;
- (iv) residency information;
- (v) health service eligibility information;
- (vi) billing information,

but does not include information that is not written, photographed, recorded or stored in some manner in a record;



Registration information as defined in regulation:

3 The following information, where applicable, relating to an individual is registration information for the purposes of section 1(1)(u) of the Act:

(a) demographic information, including the following:

- (i) name, in any form;
- (ii) signature;
- (iii) photograph or electronic image of the individual's face for identification purposes;
- (iv) personal health number or any other unique identification number that is used to identify the individual as eligible for, or a recipient of, a health service;
- (v) gender;
- (vi) date of birth;
- (vii) birth information, including
 - (A) the birth facility, and
 - (B) birth order, in the case of a multiple birth;
- (viii) marital status;
- (ix) date of death;
- (x) treaty status, including band number;
- (xi) whether the individual is a registrant or a dependant of a registrant under the Health Insurance Premiums Act;

(b) location, residency and telecommunications information, including the following:

- (i) home, business and mailing addresses, electronic address and telecommunications numbers;
- (ii) health regions, as established under the Regional Health Authorities Act, in which the individual resides and previously resided;
- (iii) citizenship or immigration status, including the date on which the individual's current immigration status expires if the individual is not a Canadian citizen or landed immigrant;
- (iv) date of entry into Canada and into Alberta;
- (v) province or country of birth or of last residence;
- (vi) date on which the individual became or expects to become a permanent resident of Canada;
- (vii) in the event the individual is registered as a registrant or dependant under the Health Insurance Premiums Act and the individual intends to be temporarily or permanently absent from Alberta,
 - (A) date of departure;
 - (B) destination and intended date of arrival at the destination;
 - (C) forwarding address;
 - (D) intended date of return, where the individual intends to be temporarily absent;
 - (E) purpose of absence;

Registration information as defined in regulation continued:

(c) health service eligibility information, including the following:

- (i) whether the individual is registered as a registrant or dependant under the Health Insurance Premiums Act;
- (ii) whether the individual is eligible to receive health services that are directly or indirectly paid for by the Government of Alberta, in full or in part;
- (iii) whether the individual has elected to opt out of the Alberta Health Care Insurance Plan and the Hospitalization Benefits Plan;
- (iv) whether the individual is exempt from the requirement to register under the Health Insurance Premiums Act;
- (v) whether the individual is exempt from the requirement to pay premiums under the Health Insurance Premiums Act;
- (vi) whether the individual is eligible to receive a reduction or waiver of premiums or charges payable in respect of health services and the level or amount, or both, of that reduction or waiver;
- (vii) information about any program of a custodian that is related to the information described in subclauses (i) to (vi), including the effective and termination dates of the program and, if applicable, the program name;

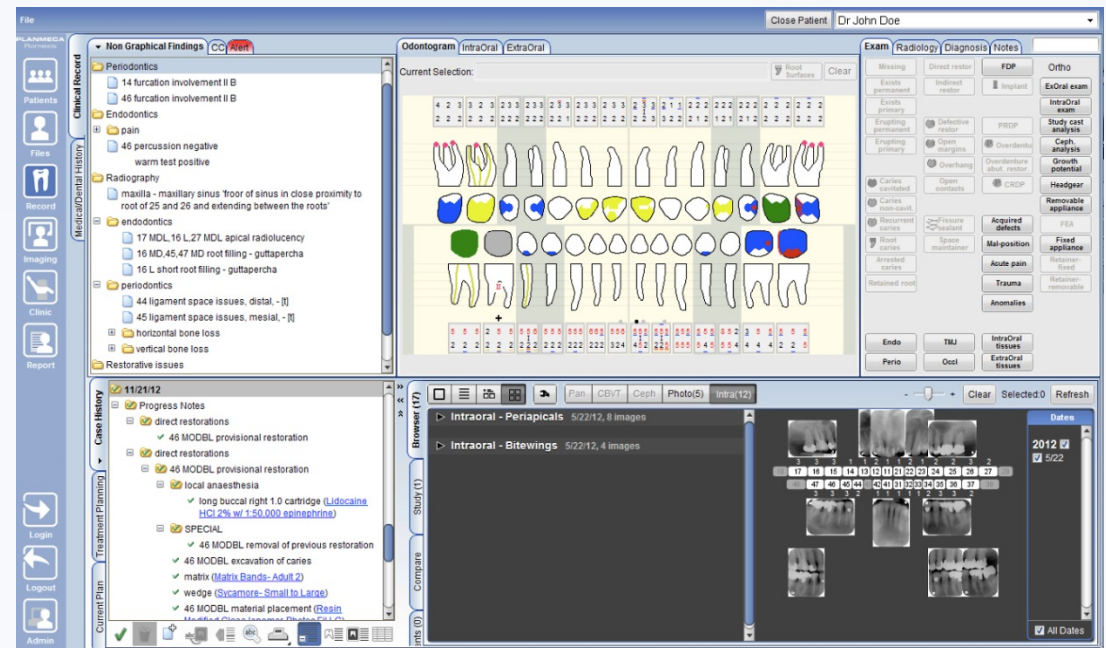
(d) billing information, including the following:

- (i) information about amounts owed by the individual to the custodian;
- (ii) method of payment;
- (iii) the individual's account number;
- (iv) if another person is liable for or will be billed for the amount owed by the individual, that person's name and account number.

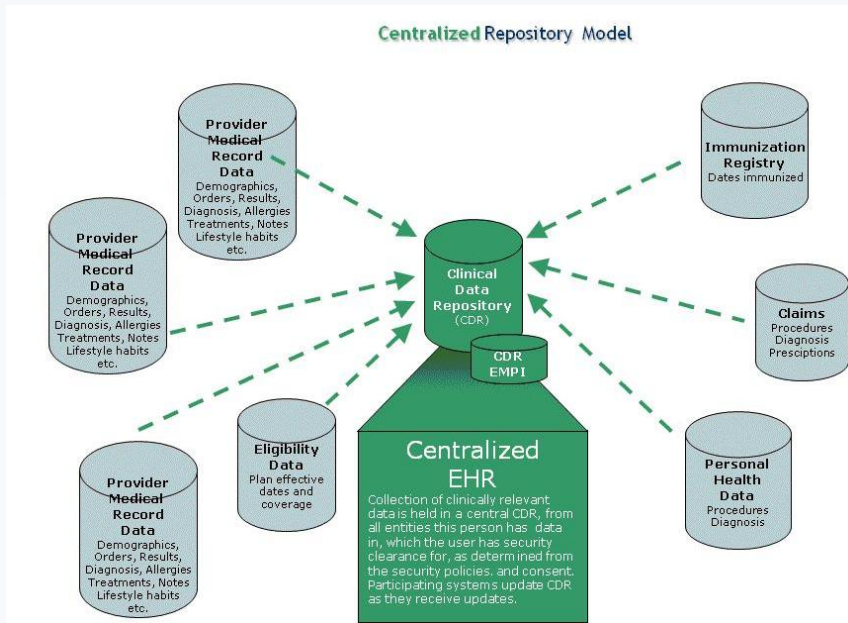
Health Information is collected in records

Health Information Act sec 1(1)(t)

“record” means a record of health information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records



Health Information is stored in repositories



Dental offices contain and use many repositories

- Paper based charts (analog)
- Employee records (analog or digital)
- Model storage (analog)
- Electronic dental records
 - File manager (word)
 - Practice Management Software
 - Third party payor communication interface
 - Diagnostic software (orthodontic tracing)
 - Image storage software (radiographs, photographs, CT scans)
 - Cad-Cam (digital impressions, 3D designed and milled prosthetics)
 - Portable electronic devices (cell phones, tablets, laptops)
 - Internal back-up (tapes, external hard drive)
 - External back-up (cloud)
 - Communications (email, web portal)
 - Others
- Alberta Netcare

In March 2011 dentists in Alberta were designated as custodians under the Health Information Act

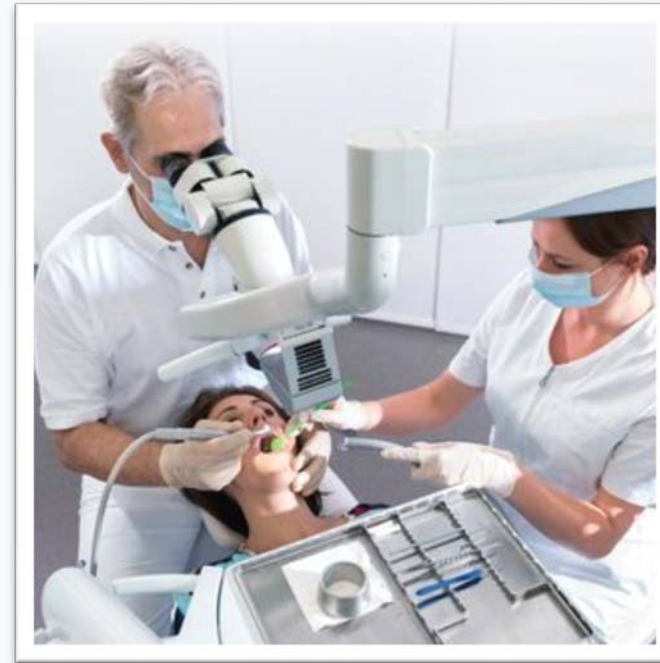
- Prior to 2011 the Personal Information and Privacy Act Alberta 2004 (PIPA) was the overlying legislation which established the rules related to privacy for dentists.
- Key difference is that PIPA is primarily consent based whereas HIA establishes authorized collection, use and disclosure conditions and rules for health information

For most of us in the room today, PIPA is the legislation that our businesses and organizations must follow when operating in Alberta except.....

..... when employed or providing services to a custodian designated under the Health Information Act

Who are custodians in Alberta?

- Chiropractors
- Optometrists
- Pharmacists
- Registered Nurses
- Denturists
- Midwives
- Opticians
- Physicians and Surgeons
- Podiatric Physicians
- Dental Hygienists
- Dentists



Why?

Under 1(1)(a) of the Health Information Act most in this room become an “affiliate” of the custodian

Health Information Act section 1(1)

In this Act,

(a) “affiliate”, in relation to a custodian, means

(i) an individual employed by the custodian,

(ii) a person who performs a service for the custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian,

(iv) an information manager as defined in section 66(1),

What are the implications of being classed as an affiliate?

Three major sections of the Health Information Act that must be aware of:

- Health Information Act Section 62(4)(a) and 62(4)(b)
- Health Information Act Section 63
- Health Information Act Section 66

Key point (Compliance)



Province of Alberta

HEALTH INFORMATION ACT

Revised Statutes of Alberta 2000
Chapter H-5

Current as of June 17, 2014

Office Consolidation

© Published by Alberta Queen's Printer

Alberta Queen's Printer
5th Floor, Park Plaza
10611 - 98 Avenue
Edmonton, AB T5K 2P7
Phone: 780-427-4952
Fax: 780-452-0668

E-mail: qp@gov.ab.ca
Shop on-line at www.qp.alberta.ca

Health Information Act section 62 (4)

Each affiliate of a custodian must comply with

(a) this Act and the regulations, and

(b) the policies and procedures established or adopted under

section 63.

Key Point

(Policies and Procedures)

63(1) Each custodian must establish or adopt policies and procedures that will facilitate the implementation of this Act and the regulations.

(2) A custodian must at the request of the Minister or the Department provide the Minister or the Department, as the case may be, with a copy of the policies and procedures established or adopted under this section.

Dr. A. Generic*
Place G Dental Centre
Place G Dental Laboratory
Suite 1 22222 3 St NW, Somewhere, AB T0Z 0Z0

*denotes professional corporation
(Dr. A. Generic Professional Corporation)

Information Privacy and Security Policies

Contact:

Dentist/ Custodian: Dr. Generic
Privacy Officer: Ms. A. Someone
Suite 1 22222 3 St NW, Somewhere, AB T0Z 0Z0
(780) 111-1111
1-877-111-1111

Key Point

(Information Manager)

66(1) In this section, “information manager” means a person or body that

- (a) processes, stores, retrieves or disposes of health information,
- (b) in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, or
- (c) provides information management or information technology services.

(2) A custodian must enter into a written agreement with an information manager in accordance with the regulations for the provision of any or all of the services described in subsection (1).

(3) A custodian that has entered into an agreement with an information manager may provide health information to the information manager without the consent of the individuals who are the subjects of the information for the purposes authorized by the agreement.

Key Point

(Information Manager continued)

- (4) An information manager to which information is provided pursuant to subsection (3) may use or disclose that information only for the purposes authorized by the agreement.
- (5) An information manager must comply with
 - (a) this Act and the regulations, and
 - (b) the agreement entered into with a custodian in respect of information provided to it pursuant to subsection (3).
- (6) Despite subsection (5)(a), a custodian continues to be responsible for compliance with this Act and the regulations in respect of the information provided by the custodian to the information manager.
- (7) A custodian that is an information manager for another custodian does not become a custodian of the health information provided to it in its capacity as an information manager, but nothing in this section prevents the custodian from otherwise collecting, using or disclosing that same health information in accordance with this Act.

Further under the Personal Information and Privacy Act:

Part 2 Protection of Personal Information

Division 1 Compliance and Policies

Compliance with Act

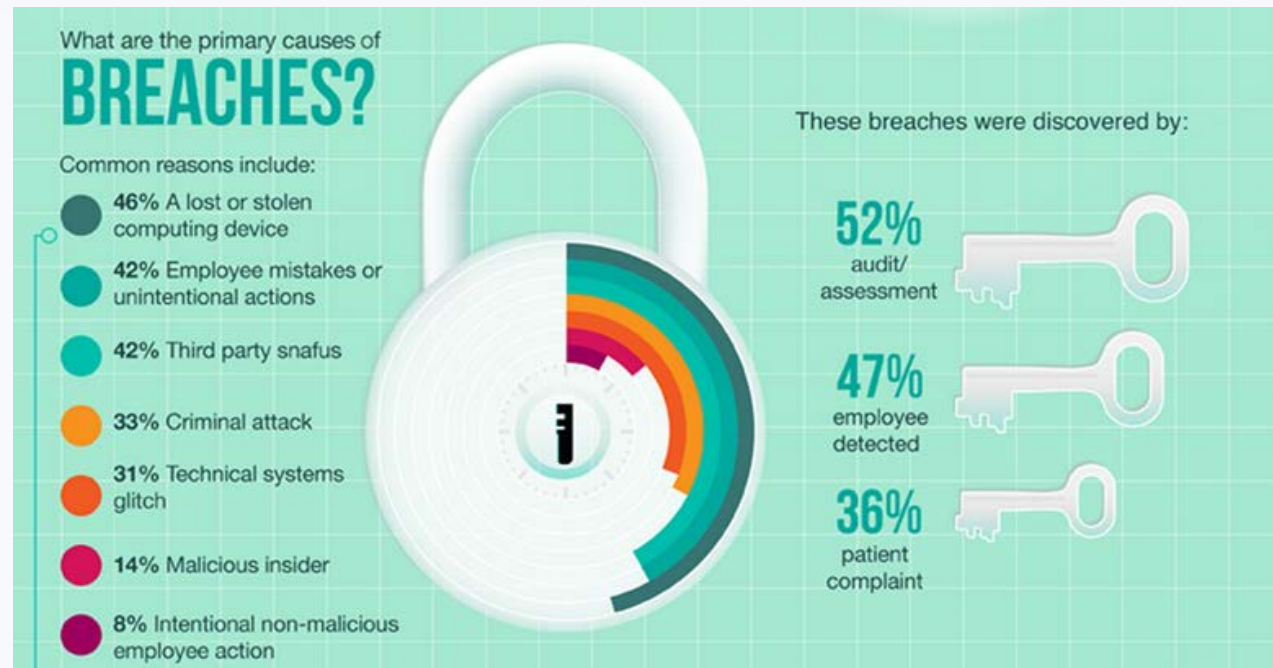
5(1) An organization is responsible for personal information that is in its custody or under its control.

(2) For the purposes of this Act, where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with this Act.

(6) Nothing in subsection (2) is to be construed so as to relieve any person from that person's responsibilities or obligations under this Act.

Contact with health information can be:

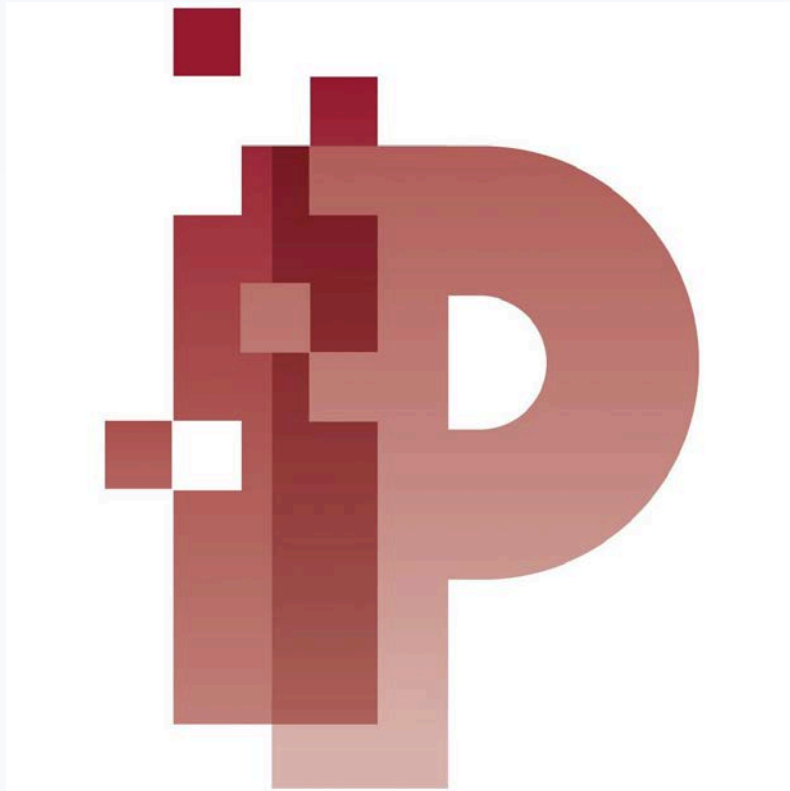
- Indirect – may come in contact with health information as part of employment or provision of service
- Direct – requires the collection, use or disclosure of health information as part of employment duties or provision of service



Ponemon Institute

Sixth Annual Study on Privacy & Security of Healthcare Data 2016

Who is responsible for regulating privacy legislation In Alberta?



Commissioner who functions within the Office of the Information and Privacy Commissioner of Alberta

Powers and duties are set out under Part 7 and Part 8 of the Health Information Act

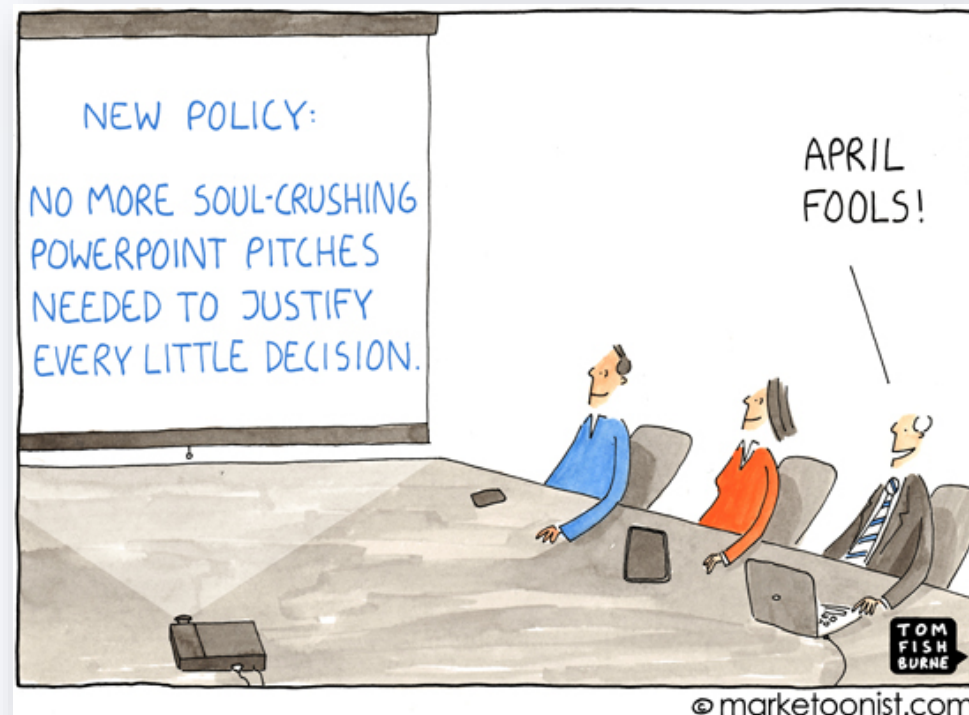
Power and duties are set out in Part 4 and Part 5 related to the Personnel Information and Privacy Act

Questions:

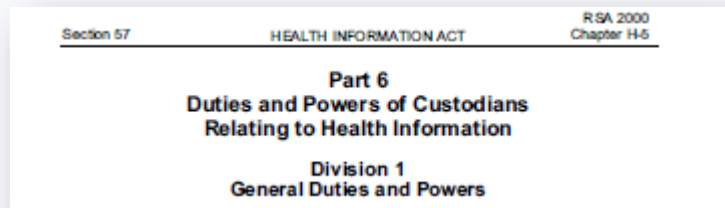
- *Are there individuals within your business or organization that would be classified as “affiliates”?*
- *Is your business or organization subject to the conditions of the Health Information Act?*



The ADA+C role is to facilitate the implementation and adoption of the requirements of the Health Information Act into Alberta dental practices



The Health Information Act establishes a set of duties that custodians and their affiliates must abide with.



- A custodian that discloses health information must make a reasonable effort to ensure that the person to whom the disclosure is made is the person intended and authorized to receive the information. (*Duty of custodian, Health Information Act Section 45*)
- Duty to consider expressed wishes of an individual who is the subject of prescribed health information* or “health information” (*Health Information Act Section 56.4 and Section 58(2)*)
- Duty to collect, use or disclose health information with highest degree of anonymity possible (*Health Information Act Section 57*)

(*prescribed health information is described under Health Information Act Section 56.1(c) and relates to information within Alberta Netcare)

Duties continued:

- Duty to collect, use or disclose health information in a limited manner (*Health Information Act Section 58*)
- Duty to protect health information (*Health Information Act Section 60*)
- Duty to ensure accuracy of health information (*Health Information Act Section 61*)
- Duty to identify responsible affiliates (*Health Information Act Section 62*)
- Duty to establish or adopt policies and procedures (*Health Information Act Section 63*)
- Duty to prepare a privacy impact assessment (*Health Information Act Section 64*)
- A custodian must enter into a written agreement with an information manager in accordance with the regulations (*Health Information Act Section 66*) provision of any or all of the services described in subsection (1).
- Duty to comply with the order of the Commissioner (*Health Information Act Section 82*)

Alberta Dental Association and College has developed a series of guides, resources and templates to assist Alberta dentists in becoming compliant with Alberta's Health Information Act

Key Points

- The requirements for Alberta dentists are not different than other custodians
- The requirements for affiliates of dentists are not different than affiliates of other custodians.
- Many of the Alberta Dental Association and College Health Information Act resources and templates mirror those developed for physicians and surgeons in concert with the *Physicians Office System Program (POSP)*
- Dental practices may represent a more complex environment (mini hospital) than other custodians
- Electronic health record requirements are the same for all custodians
- Dentists need to establish *Information Security and Privacy Policies*, obtain *information manager agreements* and ensure accepted *privacy impact assessments* are in place
- Dentists came under the Act in 2011 and catch-up is required

Dentists have met resistance from the supporting dental industry in relation to obtaining the necessary agreements and ensuring products or services meet the expected standards as required under the Health Information Act

- Mixed messaging as to what is required in relation to privacy impact assessments, information manager agreements, contractor agreements, electronic health record system requirements
- Delays have legal, ethical and reputation implications for dentists and the supporting dental industry
- Delays will have an impact on patient health

Starting Point to move forward together

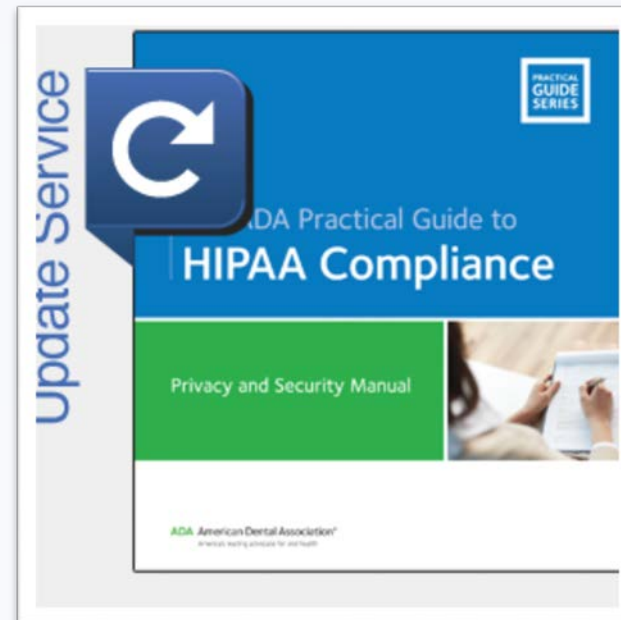
What about HIPAA Compliance?

Not the same as HIA

Privacy requirements are jurisdiction specific and while common principles there are differences

Custodians, business, organizations and individuals need to ensure that the products and services meet the requirements within the jurisdiction used or provided

Having an accepted Privacy Impact Assessment in place avoids unwanted surprises and costs



What class of “affiliates” does your business or organization represent?

- Staff of custodian - direct

Dentists, Dental Hygienist, Nurses (custodians but may be working in an affiliate relation)

Receptionist, office manager, dental assistants, treatment coordinators, sterilization technicians, students

- External service providers

Custodial, facility management, security, equipment repair, product or company sale representative, dental laboratories, privacy consultants

- Information Managers

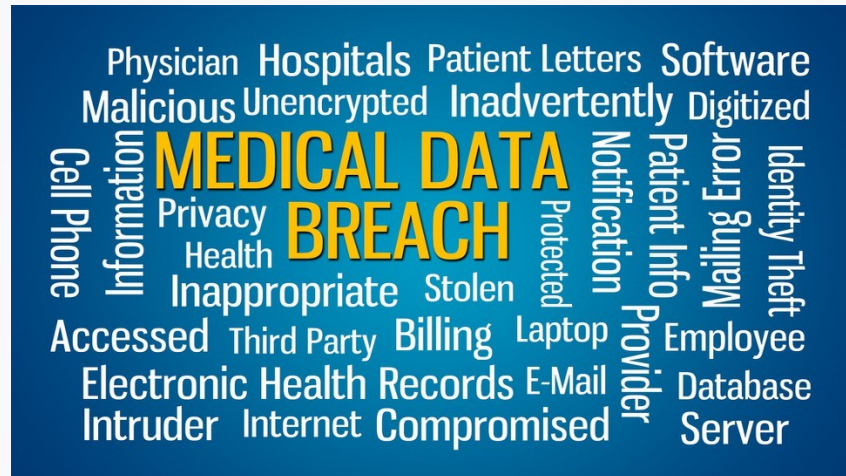
IT services, secure email or web services, remote off-site back-up (cloud), practice management software support, digital imaging support, record destruction, health benefit claim transmission

•

All affiliates need to abide by the Health Information Act and the policies and procedures of the custodian

- Common template developed by the Alberta Dental Association and College for dental practices
 - Not all of the policy sections apply to affiliates
 - Adopt policies and procedures of the custodian related to health information as it relates to affiliates
- Other Options
 - Establish policies and procedures consistent with the Health Information Act for your business or organization
 - Provide them to the custodian for review
 - Custodian will need to decide if they are similar
 - What would be looking for are administrative, technical and security including training provisions that are consistent with those of the custodian
 - Custodian will provide them to the Office of the Information and Privacy Commissioner as part of Privacy Impact Assessment submission for review to determine if shortcomings

Important to
remember why



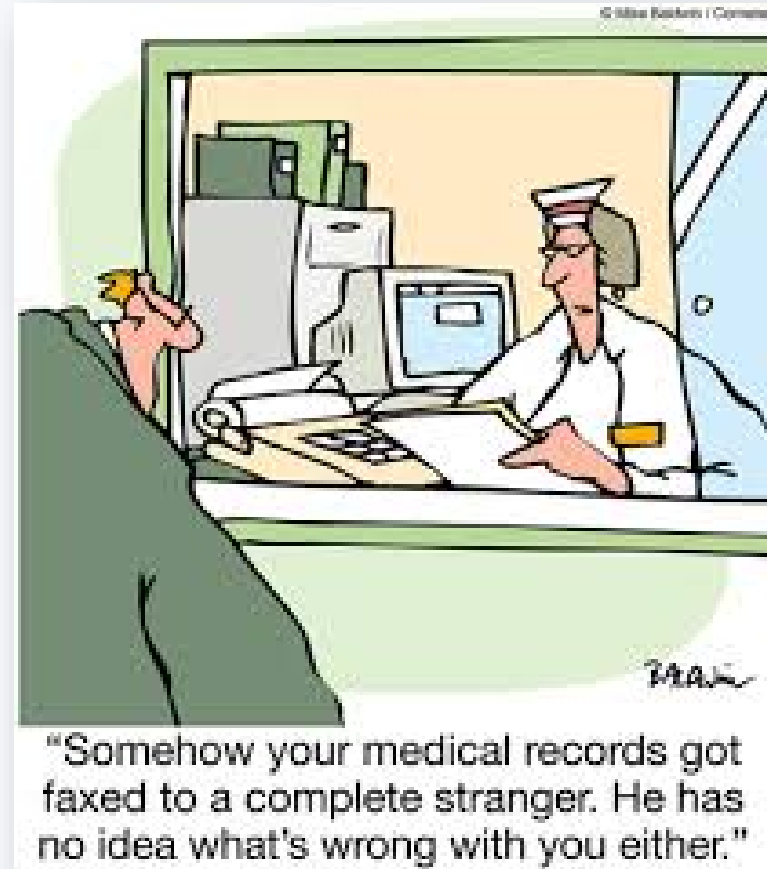
Health Information Act section 62

(2) Any collection, use or disclosure of health information by an affiliate of a custodian is considered to be collection, use or disclosure by the custodian.

(3) Any disclosure of health information to an affiliate of a custodian is considered to be disclosure to the custodian.

Confidentiality, Privacy and Security

Is there a difference?



QuickPoint:

Maintaining privacy means more than just safeguarding confidentiality – it is an ongoing program that involves accountability, control of information flow, right of access procedures, and security measures.

Information Security and Privacy

Health Information Act:

Duty to protect health information

60(1) A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will

(a) protect the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information,

(b) protect the confidentiality of health information that is to be stored or used in a jurisdiction outside Alberta or that is to be disclosed by the custodian to a person in a jurisdiction outside Alberta and the privacy of the individuals who are the subjects of that information,

(c) protect against any reasonably anticipated

(i) threat or hazard to the security or integrity of the health information or of loss of the health information, or

(ii) unauthorized use, disclosure or modification of the health information or unauthorized access to the health information, and

(d) otherwise ensure compliance with this Act by the custodian and its affiliates.

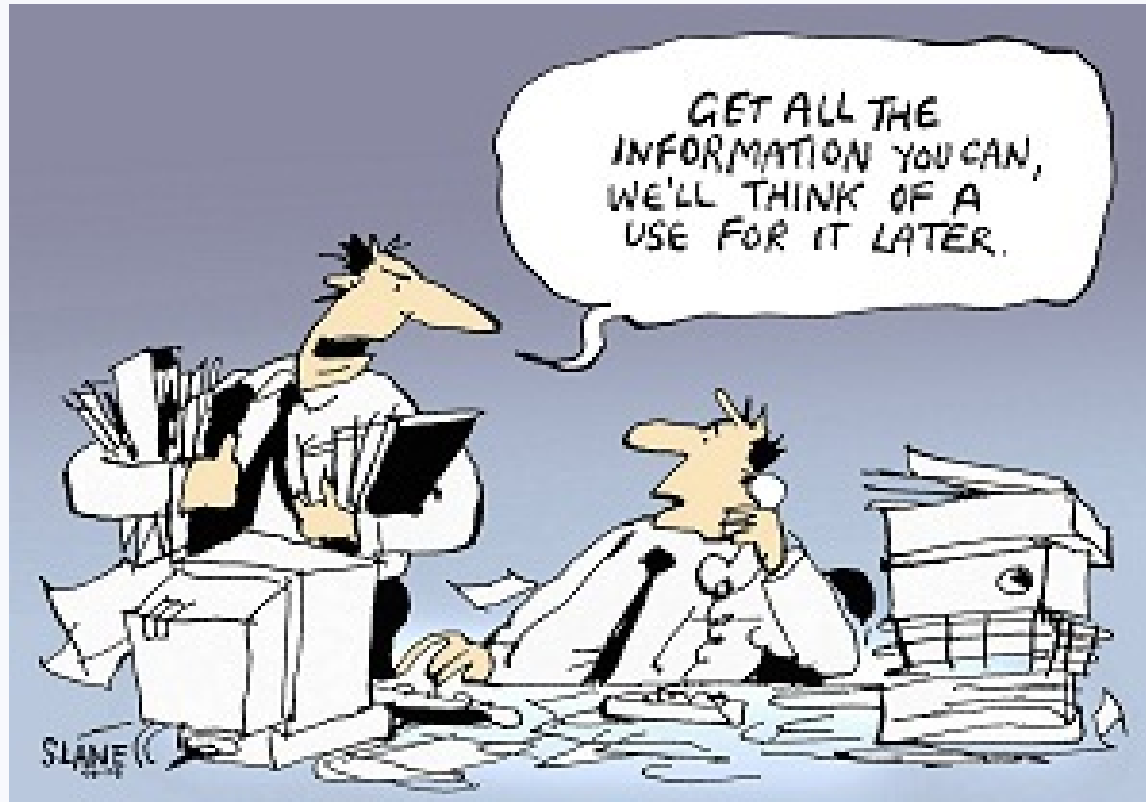
Why would a dentist ask you to sign a confidentiality oath or contractor agreement?

- Administrative Safeguard
- Provides a records that affiliates have been made aware of the need to comply with the Health Information Act and regulations plus the policies and procedures of the custodian
- Training and awareness is identified
- Consistent with *Duty to protect health information* as noted in Health Information Act Section 60
- Consistent with *Security of health information* Health Information Act Health Information Regulation Section 8
- Who should sign?
 - Individual
 - Company
 - Depends on circumstances
- Not mandatory requirement under the HIA but strongly advised
 - Template agreements available

Case Scenario

- Company J provides janitorial and custodial services
 - Building manager contracts Company J to clean common premises and those under lease
 - Doctor X is a custodian and the lease agreement includes janitorial services for the premises occupied where health information is collected, used, disclosed and stored
- What agreements should be in place?
 - Who should the agreements be with?
 - Who is responsible for training and compliance monitoring?

Information Manager Agreements



Information Manager Agreements

Administrative Safeguard as part of a risk assessment process

Related to many of the duties of a custodian

Written agreement between a custodian and an affiliate who is identified as an information manager under the Health Information Act sec 66

Must conform with the requirements as outlined in Section 7.2 of the Health Information Act Health Information Regulation

Mandatory

Template agreement available that incorporate custodian's privacy policies but may not be the only option



Information manager agreement (Health Information Act Health Information Regulation)

7.2 For the purposes of section 66(2) of the Act, an agreement between a custodian and an information manager must

- (a) identify the objectives of the agreement and the principles to guide the agreement,
- (b) indicate whether or not the information manager is permitted to collect health information from any other custodian or from a person and, if so, describe that health information and the purpose for which it may be collected,
- (c) indicate whether or not the information manager may use health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be used,
- (d) indicate whether or not the information manager may disclose health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be disclosed,
- (e) describe the process for the information manager to respond to access requests under Part 2 of the Act or, if the information manager is not to respond to access requests, describe the process for referring access requests for health information to the custodian itself,
- (f) describe the process for the information manager to respond to requests to amend or correct health information under Part 2 of the Act or, if the information manager is not to respond to requests to amend or correct health information, describe the process for referring access requests to amend or correct health information to the custodian itself,
- (g) describe how health information provided to the information manager is to be protected, managed, returned or destroyed in accordance with the Act,
- (h) describe how the information manager is to address an expressed wish of an individual relating to the disclosure of that individual's health information or, if the information manager is not to address an expressed wish of an individual relating to the disclosure of that individual's health information, describe the process for referring these requests to the custodian itself, and
- (i) set out how an agreement can be terminated.

Use of health information by information managers

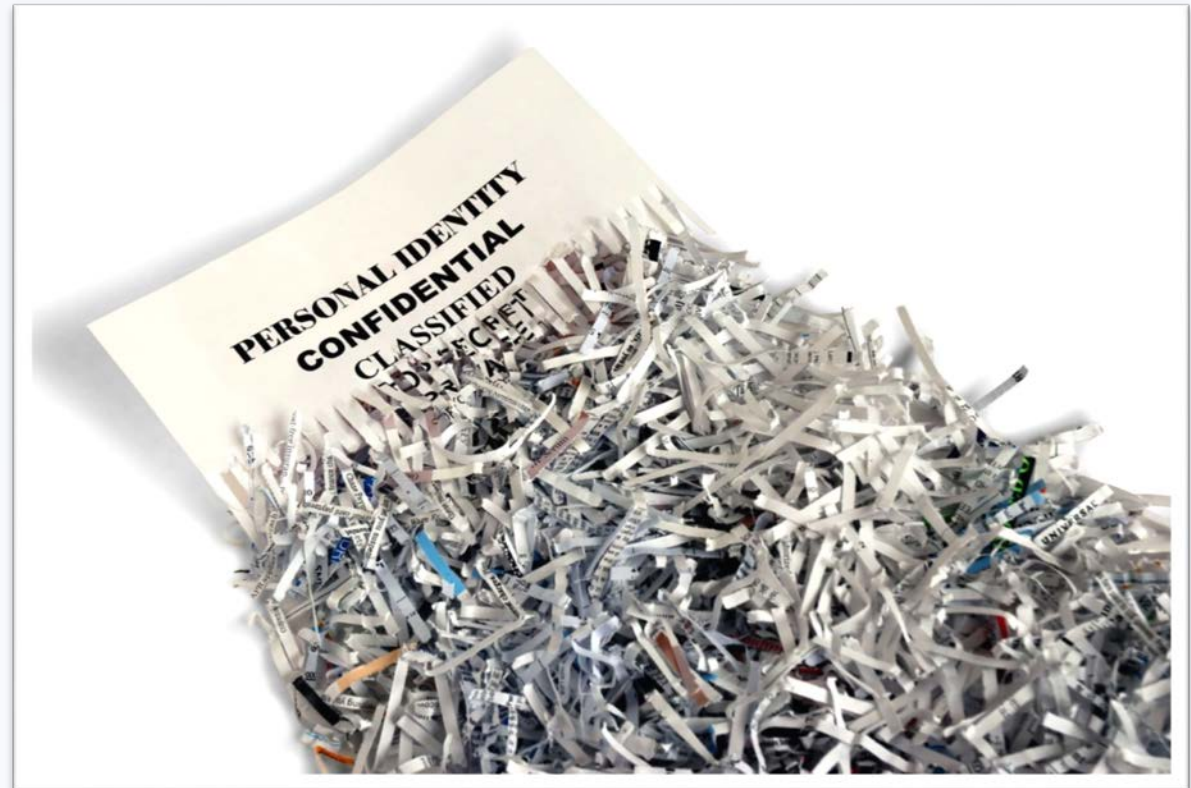
Bug fixes, trouble shooting even if health information is encrypted is a “use”

Storage of health information is a “use” even if transient, short term and encrypted

Help desk or technical support requiring access to patient health information is a use

Destruction of records is a use

System maintenance, design, testing and upgrading that involves real data is a use



There are additional requirements for health information that is stored or used in a jurisdiction outside of Alberta

- Administrative Safeguard as part of risk assessment process
- Related to many of the duties of a custodian
- Must conform with the requirements as outlined in Section 8(4) of the Health Information Act Health Information Regulation
- Usually captured through additional provisions within information manager agreement
- Mandatory
- Template agreement available that incorporate custodian's privacy policies but may not be the only option



What must be addressed when health information is to be stored or used in a jurisdiction outside of Alberta? (Health Information Act Health Information Regulation sec 8(4))

(4) In order to ensure the privacy and confidentiality of health information that is to be stored or used by a person in a jurisdiction outside Alberta or that is to be disclosed to a person in a jurisdiction outside Alberta, the custodian must, prior to the storage, use or disclosure of the information, enter into a written agreement with the person that

- (a) provides for the custodian to retain control over the health information,
- (b) adequately addresses the risks associated with the storage, use or disclosure of the health information,
- (c) requires the person to implement and maintain adequate safeguards for the security and protection of the health information,
- (d) allows the custodian to monitor compliance with the terms and conditions of the agreement, and
- (e) contains remedies to address any non-compliance with or breach of the terms and conditions of the agreement by the other person.

What are alternatives to using information manager agreement template?

Two issues that must be addressed

First:

1. Does the agreement cover the required elements?
2. Do the privacy policies that underlie the agreement meet the requirements of the Health Information Act?

Second:

1. There will be the need for a review of the agreement and/or policies by the custodian prior to submission to the Office of the Information and Privacy Commissioner
2. A privacy impact assessment will be submitted by the custodian to the Office of the Information and Privacy Commissioner which will include the information manager agreement and privacy policies to ensure that they are consistent with the obligations under the Health Information Act and regulations

Options, issues and implications discussion

- Customize the template ensuring that those clauses consistent Section 7.2 and 8(4) of Health Information Act Health Information Regulation are maintained
- Develop information manager agreement or contract that incorporate clauses that address Section 7.2 and 8(4) of Health Information Act Health Information Regulation
- Map terms of use agreement and privacy compliance policies to Section 7.2 and 8(4) of Health Information Act Health Information Regulation

Case scenario

Dental practice wants to install a video surveillance security system

The system would monitor external, public, internal and restricted areas of the practice

The custodian is considering either a self monitored system or contracting the service of a security company

- Is a privacy impact assessment required?
- Is a new repository that contains health information created?
- Is an information manager agreement required?
- Whose information privacy and security policies need to be followed?
- Is the consent of the patient required if the video surveillance is in an operator (treatment area)
- How long would the video surveillance records need to be kept before destruction?

Case scenario

- Dental practice wants to switch from film based to digital radiography
- Dental Supply Company ABC with an office in Somewhere, Ab sells the software and hardware
- Dental Supply Company ABC installs the software and hardware
- Dental supply company ABC provides warranty and ongoing maintenance of the hardware
- Software support is provided by the manufacture, Digital Systems through remote access to the custodian's server that involves disclosure and use of health information from support desk in Someplace USA

Assumption: Accepted PIA from the OIPC in place prior to installation due to creation of a new repository in the existing EHR

- What would the OIPC expect to see in the PIA submission for it to be accepted?
 - A confidentiality or contractor agreement in place for the installation and ongoing hardware maintenance with Company ABC or service technicians?
 - A information manager agreement in place with Company ABC or manufacture, Digital Systems?
 - Privacy policies of the custodian? Company ABC? Digital Systems?

Consequences:

- What are implications for a custodian if not being able to obtain an information manager agreement?

Electronic Health Record System Requirements



Common misnomer:


Electronic health (dental) record systems by definition are not just practice management software

They consist of many repositories with associated software that may be integrated, bridged, linked or stand alone that lie on internal servers, external servers or portable devices.

Electronic dental record systems include:

- File manager (word)
- Practice Management Software
- Third party payor communication interface
- Automated appointment scheduling and confirmation
- Diagnostic software (orthodontic tracing)
- Image storage software (radiographs, photographs, CT scans)
- Cad-Cam (digital impressions, 3D designed prosthetics)
- Portable electronic devices (cell phones, tablets, laptops)
- Internal back-up (tapes, external hard drive)
- External back-up (cloud)
- Communications (secure email, web portal)
- Alberta Netcare
- Other

System collectively must have reasonable safeguards in place



Guidance for Electronic Health Record Systems

Under the [Health Information Act \(HIA\)](#), custodians and their information managers must take reasonable steps to protect health information against threats to confidentiality or security in electronic health record (EHR) systems, including unauthorized access, use, disclosure, modification or loss of health information.

Purposes

This document is meant for custodians and their information managers (i.e. EHR service providers) to assess the safeguards in EHR systems.

Specifically, you may use this document for the following three purposes:

- To assess whether EHR systems comply with HIA and meet the OIPC's expectations for protecting health information with reasonable safeguards.
- To support the submission of a **Privacy Impact Assessment (PIA)** on an EHR system to the Office of the Information and Privacy Commissioner (OIPC). OIPC staff assigned to review a custodian's PIA may ask that a gap analysis against these guidelines be completed if further information is needed to complete a PIA review.
- To prepare PIA amendments or for continuous improvement to ensure upgrades or changes to systems comply with HIA requirements.

This document is an administrative tool intended to assist custodians in understanding the *Health Information Act* (HIA). This document is not intended as, nor is it a substitute for, legal advice. For the exact wording and interpretation of HIA, please read the Act and its regulation in their entirety. This document is not binding on the Office of the Information and Privacy Commissioner of Alberta.

This guidance may be used voluntarily to assess your EHR. It does not replace the OIPC's PIA Requirements or Alberta Health's Provincial Organizational Readiness Assessment (pORA), which are both mandatory under HIA.

When using this guidance, you will likely need to work with your EHR service provider (i.e. information manager) to fully understand and complete an assessment.

June 2016

Page 1 of 16

Gap analysis

Current State

- Individual access controls not in place
- Audit function minimal
- Information manager agreements not in place
- Use of unsecure email
- System upgrade or new installation without having an accepted privacy impact assessment in place
- Servers not in restricted locked area
- Back-up of the entire electronic health record system is not occurring
- Administrative, technical and security provisions are weak
- Encryption not being used (communication, portable devices)
- Business continuity is at risk as anticipated threats to security, integrity, or loss of health information are not in place
- Policies for information security not in place
- Policies for conversion of analog health records to digital not in place



Audit function requirements for Electronic Health Record Systems under the Health Information Act

Not a different situation in the United States:

164.312 Technical safeguards

(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Health Information Act Electronic Health Record Regulation

Logging capacity required

6(1) A custodian must ensure its electronic health record information system creates and maintains logs containing the following information:

- (a) user identification and application identification associated with an access;
- (b) name of user and application that performs an access;
- (c) role or job functions of user who performs an access;
- (d) date of an access;
- (e) time of an access;
- (f) actions performed by a user during an access, including, without limitation, creating, viewing, editing and deleting information;
- (g) name of facility or organization at which an access is performed;
- (h) display screen number or reference;
- (i) personal health number of the individual in respect of whom an access is performed;
- (j) name of the individual in respect of whom an access is performed;
- (k) any other information required by the Minister.

(2) This section applies only to electronic health record information systems established after the coming into force of this section.

Case scenario

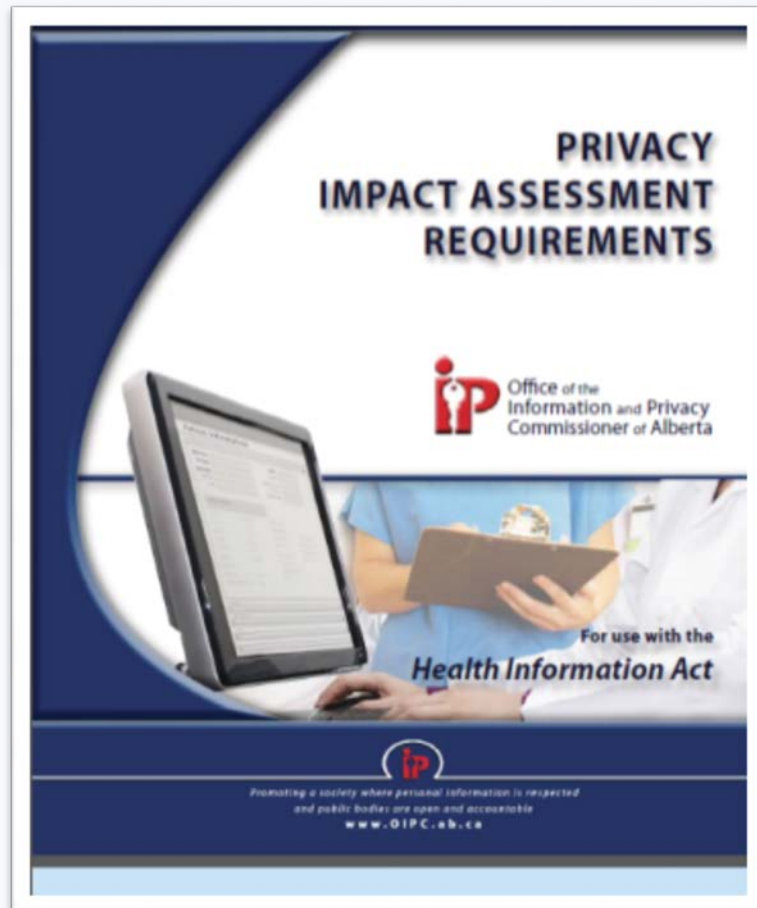
- Doctor X has a legacy based practice management software that is only used for patient billing and appointment scheduling that has not been upgraded, has minimal auditing capacity, uses a common password and has a support contract from the software vendor that includes remote access to the server
- Dr X has not used or activated other practice management modules that were available for recording diagnostic, treatment and care information
- Dr X decides he wants to begin using these functions

- Are changes required to the existing practice management software in use even if Doctor X does not proceed with activating additional modules?
 - What about access controls?
 - Regardless of system age, should unique individual user access be required?
 - Is an information manager agreement required with the software vendor?
 - Is there a minimum level of auditing capacity that should be in place?

Doctor X decides to activate modules

- What steps must be followed and what needs to be changed within the practice management software?
 - Is a PIA submission required?
 - Is an IMA required?
 - Can the use of the single common password continue?
 - Do auditing provisions need to be upgraded to those outlined under the Electronic Health Record Regulation?

Mandatory Privacy Impact Assessment Requirements under the Health Information Act



Health Information Act

Duty to prepare privacy impact assessment

64(1) Each custodian must prepare a privacy impact assessment that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual who is the subject of the information.

(2) The custodian must submit the privacy impact assessment to the Commissioner for review and comment before implementing any proposed new practice or system described in subsection (1) or any proposed change to existing practices and systems described in subsection (1).

Alberta Dental Association and College has been working with Alberta Health and the Office of the Information and Privacy Commissioner on the format, structure and content of Privacy Impact Assessments

Current Pathway

- Initial Dental Practice PIA (policy and system review)
- Expedited Alberta Netcare PIA (includes PORA)
- Amendments or additional PIAs as required under HIA Sec 64

Optional pathway to expedite Alberta Netcare implementation currently *under discussion and consideration*

- Privacy and Information Security Policy PIA
- Alberta Netcare Expedited PIA (includes PORA)
- System or component based PIAs
- Amendments or additional PIAs as required under HIA Sec 64

What constitutes a new or change to administrative practice or information system?

Yes or Maybe?

- Adding Modules
- Additional functionality within software
- Software version change
- Changing operating system
- New custodian
- Creation of repository or change to existing repository
- Changes post March 2011
- New office

No

- Not bug fixes
- New fee guide update

❖ Important Note: When in doubt contact the Office of the Information and Privacy Commissioner for advice

Case Scenario

A module to an existing practice management software* is added which allows for automated telephone, email or text reminders of appointments to be sent

**Assumption is that the existing practice management software is a legacy system (pre 2011) and has undergone only software bug fixes and annual fee guide updates*

What are the implications of adding new functionality to a legacy system?

- IMA required?
- PIA required?
- Audit functions?
- Consent required to contact patient?

Case Scenario

- Dental practice has an existing digital radiography system but wants to change to different software to capture and store images
- Dental practice wants to change to a different secure email provider

Is a new PIA or amended PIA required before using the service or software?

- Why?
 - New repository
 - New IMA
 - Audit functions

Case Scenario

Dental practice wants to convert analog health records to digital and destroy originals



What is required?

- Custodian must have policy and procedures in place for record conversion and destruction (Health Information Act and Alberta Dental Association and College Standards of Practice)
- If using external contractors for either conversion or destruction will require IMA to be obtained
- Submit a PIA to the Office of the Information and Privacy Commissioner
- Once accepted PIA obtained, conversion process can start

Alberta Netcare: short and long term implications for the dental profession



- Dentists, along with chiropractors and optometrists are new authorized custodians
- Dentists can voluntarily gain access to Alberta Netcare
- Must have an existing PIA in place, submit an expedited PIA for access to Alberta Netcare, complete a Provincial Organizational Readiness Assessment (p-ORA), sign an information manager agreement with Alberta Health plus training and a site visit
- Web portal access only

What is the future and where are we headed?

Short term

- e-prescribing
- diagnostic imaging from dental practices entered into Alberta Netcare
- patient care decisions based collectively on health information within Alberta Netcare and the dental practice
- patient access to their own health information via the Personal Health Portal (MyHealth.Alberta)

Medium term

- specific diagnosis, treatment and care information entered into Alberta Netcare from dentists

Longer term

- total integration of Alberta Netcare and dental practice electronic health record systems



The Health Information Act facilitates the future!

Family and Children's Dentistry

CONSENT FOR USE AND DISCLOSURE OF HEALTH INFORMATION

SECTION A: PATIENT GIVING CONSENT

Name: _____
Address: _____
Telephone: _____ E-mail: _____
Patient Number: _____ Social Security Number: _____

SECTION B: TO THE PATIENT—PLEASE READ THE FOLLOWING STATEMENTS CAREFULLY.

Purpose of Consent: By signing this form, you will consent to our use and disclosure of your protected health information to carry out treatment, payment activities, and healthcare operations.

Notice of Privacy Practices: You have the right to read our Notice of Privacy Practices before you decide whether to sign this Consent. Our Notice provides a description of our treatment, payment activities, and healthcare operations, of the uses and disclosures we may make of your protected health information, and of other important matters about your protected health information. A copy of our Notice accompanies this Consent. We encourage you to read it carefully and completely before signing this Consent.

We reserve the right to change our privacy practices as described in our Notice of Privacy Practices. If we change our policy,

Contact Person: Pamela Allred
Telephone: (404) 349 - 7777 Ext 105 Fax: (404) 349 - 8459
E-mail: fcdentistry@earthlink.net
Address: 2440 Fairburn Road, Suite 301, Atlanta, Georgia 30331

Right to Revoke: You will have the right to revoke this Consent at any time by giving us written notice of your revocation submitted to the Contact Person listed above. Please understand that revocation of this Consent will not affect any action we took in reliance on this Consent before we received your revocation, and that we may decline to treat you or to continue treating you if you revoke this Consent.

SIGNATURE

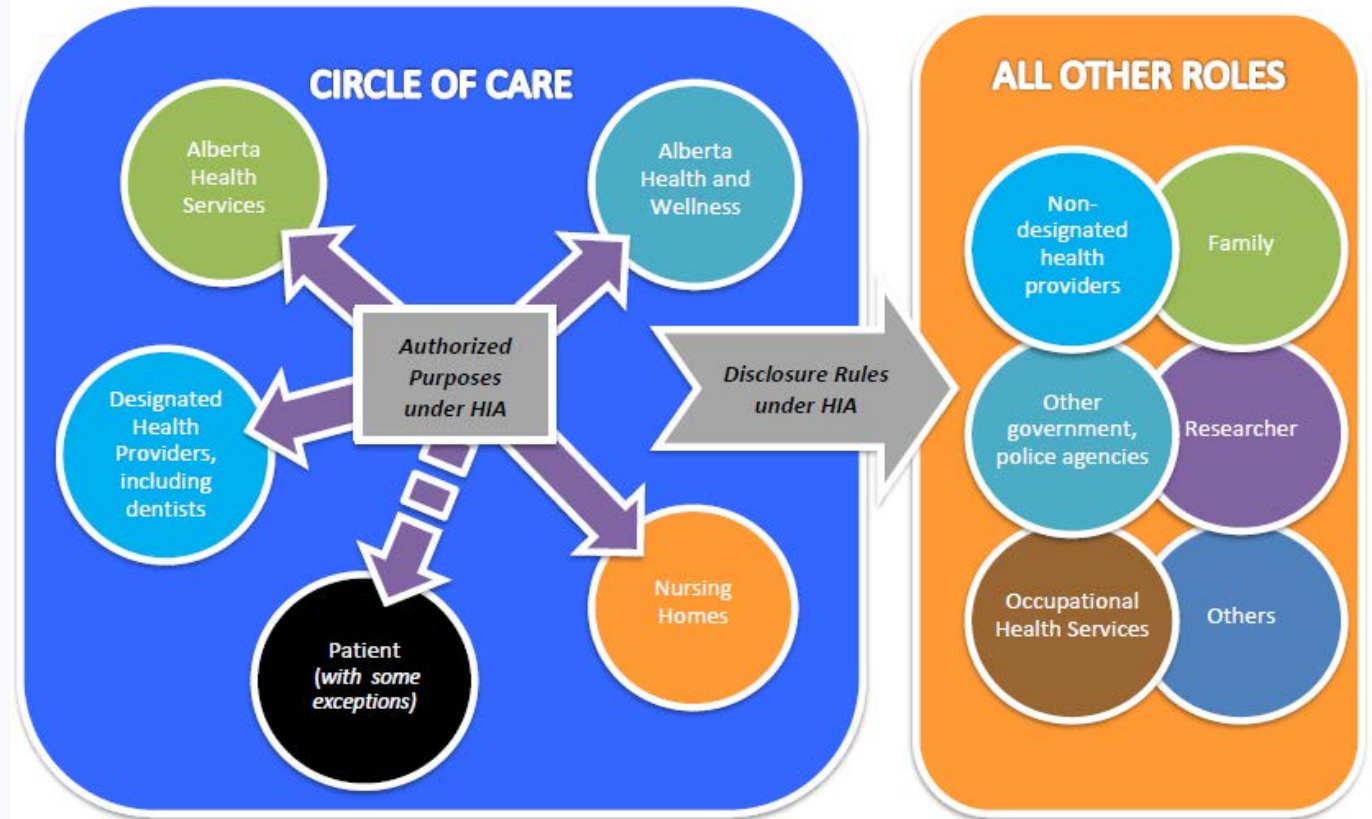
I, _____, have had full opportunity to read and consider the contents of this Consent form and your Notice of Privacy Practices. I understand that, by signing this Consent form, I am giving my consent to your use and disclosure of my protected health information to carry out treatment, payment activities and health care operations.

Signature: _____ Date: _____

If this Consent is signed by a personal representative on behalf of the patient, complete the following:

Personal Representative's Name: _____
Relationship to Patient: _____

"With a Lott of Love"





Additional tools in development

- Advisory letter from the Office of the Information and Privacy Commissioner of Alberta related to requirements of the Health Information Act for supporting dental industry
- Templates refinements and additional templates as identified
- Guide for Privacy Impact Assessment submissions for dentists
- Alberta Netcare resources for dentists
- Proposed listing service, technology and products report related to Health Information Act requirements and the existence of accepted Privacy Impact Assessments from the OIPC for members of the Alberta Dental Association and College



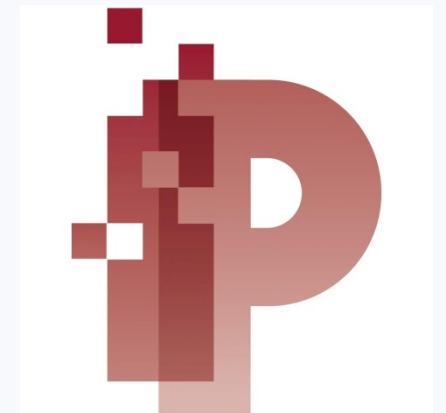


DRAFT: Proposed listing service, technology and products report related to Health Information Act requirements and the existence of accepted Privacy Impact Assessments from the OIPC for members of the Alberta Dental Association and College

Service, technology or product	Company or Individual	Contact name	Address	Email/telephone	Contractor Agreement or Confidentiality Oath	Information Manager Agreement	Terms of Use	Privacy Policies	Audit Logs	Access Controls	Meets HIA Req.
Remote Backup	Cloud One	Joe Smith	11 Rd, Someplace Ontario X0X 0X0	jsmith@cloudone.ca 416-111-1111	N/A		Not consistent with HIA, sec 7.2 and 8(4) deficiencies	Company, Consistent with PIPEDA but HIA uncertain		Unique User ID and Password	Maybe, ?
Practice Management Software	Dental First	Bill Smith	22 St, Somewhere Alberta T0T 0T0	bsmith@dentalfirst.ca 780-222-2222	N/A	Yes		Company, Consistent with HIA	Yes	Unique User ID, Password, Fob	Yes
Records Destruction	Shred Best	Mary Smith	33 Ave, Something, Alberta T1T 1T1	msmith@shredbest.ca 403-333-3333	N/A	Yes		Custodians			Yes
Janitorial	Clean Best	Jill Smith	44 Cres, Everywhere, Manitoba Z4Z 4Z4	jsmith@cleanbest.ca 204-444-4444	Contractor Agreement	N/A		Company, Consistent with HIA			Yes
Equipment Repair	Fixed Right	Bob Smith	55 Blvd, Nowhere, Alberta T5T 5T5	bmsmith@fixedright.ca 780-555-5555	Confidentiality Oath	N/A		Custodians			Yes
Encrypted Email and Secure Web Portal	Com Secure	Carol Smith	66 Highway, Bestplace, USA	csmith@comsecure.com 702-666-6666			HIPAA	Company HIPAA		Unique User ID and Password	*
* Company or individual has not demonstrated prepared to work with custodian to meet Health Information Act requirements					? Company or individual working with custodian but outcome unknown		Yes Custodian have accepted PIA related to this product, service or technology				



Special thank you to Silvia Russell,
Nji Lionel Nji, Brian Hamilton and
of course all of you for attending!



Electronic copies of this presentation can be obtained by contacting Jodi Wilkinson at jwilkinson@adaandc.com

Alberta Dental Association and
College
Suite 101, 8230 – 105 Street
Edmonton, Alberta T6E 5H9

Phone: (780) 432-1012
Fax: (780) 433-4864
Toll Free (within Alberta) 1-800-843-3848

Email: reception@adaandc.com

