alberta dental association & college

Guide for Implementing the Requirements of the Health Information Act

Table of Contents

Introduction

Alberta's *Health Information Act* is privacy legislation that sets out specific rules about the collection, use, disclosure and protection of the health information that all dentists, have in their custody and control. Dentists in Alberta are required to comply with the Alberta *Health Information Act* and in order to do so, need to go beyond just protecting patient's confidentiality, dentists also need to develop and participate in an ongoing privacy program that addresses accountability, information flow, right of access, and security. Alberta dentists must be compliant with the *Health Information Act*, which is administered by the Office of the Information and Privacy Commissioner of Alberta.

The requirements for how dentists collect, use, disclose and protect health information have changed as dentists are now governed by Alberta's *Health Information Act* (HIA) as of March 1, 2011. The HIA is much more than privacy legislation. It is enabling legislation along with the Health Professions Act and Government Organization Act that defines the legal parameters that allow dentists to provide health care to our patients.

The Alberta Dental Association and College has developed a series of Guides supported by resources and templates to assist Alberta dentists to implement a privacy and confidentiality program that is compliant with Alberta's *Health Information Act* and the Alberta Dental Association and College Standard of Practice: Privacy and Management of Patient Health Information. The Guides with their associated resources are organized in a Step-by-Step approach.

This **Guide for Implementing the Requirements of the Health Information Act** represents **Step 2** in the process. This document provides a summary and explanations of the steps involved in the development and implementation of a Privacy and Security Program for a dental practice.

The previous step was to create an understanding of the Act and its associated regulations for the custodian (dentist) and staff (affiliates). This was accomplished through review of the Alberta Dental Association and College **Standard of Practice: Privacy and Management of Patient Health Information** and the **Guide for the Alberta Health Information Act: Privacy and Management of Patient Health Information.** In addition, familiarizing and developing a working knowledge of the *Health Information Act* and associated regulations is required.

A. Overview: Guide for Implementing the Requirements of the Health Information Act

A dentist in Alberta is required to comply with the *Health Information Act* and in order to do so, dentist's need to go beyond just protecting the patient's confidentiality, dentists also need to develop and participate in an ongoing privacy program that addresses accountability, information flow, right of access and security. The following outlines the sequence required to implement a privacy program:

1. **Complete Step 1:** Development of an understanding of the *Health Information Act* and associated regulations through review of the Alberta Dental Association and College **Standard of Practice: Privacy and Management of Patient Health Information** and the **Guide for the Alberta Health Information Act: Privacy and Management of Patient Health Information.** In addition, familiarizing and developing a working knowledge of the *Health Information Act* and associated regulations is required.

2. **Start Step 2:**

2.1. Read the Guide for Implementing the Requirements of the Health Information Act

2.2. Assemble a team or consider appointing a Privacy Officer at this stage

2.2.1. While it is the custodian's responsibility to undertake the evaluation of a practice, doing this as a team leads to a much greater understanding of responsibilities and the current situation.

2.2.2. It is not necessary to appoint a Privacy Officer at this point but there may be merit in doing so. It can lead to an early assignment of responsibilities and follow through on required tasks. In some cases, a Privacy Officer may be in place and they will need to ensure that existing policies and protocols are compliant as is a mandated under the Act.

2.2.3. The custodian must identify its affiliate who will be responsible for ensuring that the ACT, the regulation and policies and procedures are complied with (Privacy Officer). As the custodian is ultimately responsible for the Practice Privacy and Security Policy and Protocols under the Act it is possible for the custodian to assume this role but this would be unusual.

2.3. Use the Resource Templates

Evaluating the dental practice privacy and management of health information program involves conducting a self-assessment of the current state of the practice in the collection, accountability, information flow, right of access, and security of health information. This type of assessment can be used to determine which areas of the practice require improvement to better comply with provisions regulating the collection, use, disclosure, retention and destruction of personal health information. **Complete** the evaluations, reviews and questionnaires. The results of the overall assessment; an evaluation of the current state compared with the expected standards, will help to develop a plan to manage the privacy of personal information in the practice.

2.3.1. **The Site Privacy and Security Inspection:** This is used to assess the current status of privacy practice and protection in specific areas of each dental office. Since most

dental offices have similar spaces, there are examples provided of the information that is being looked for. This should help offices customize these pages to represent the situation within a particular practice.

2.3.2. **The Health Information Registry:** This relates to what health information dentists have and how it is handled. It provides a basic description of health information in the dental practice organized by function. (Ex. Patient files, practice billing system). Again, an example has been given to follow through and an office should be able to look at this and adopt what is appropriate and customize the rest.

2.3.3. **Practice Privacy Assessment:** This **identifies** how and how well the dental practice currently meets the Standard and, if there are significant gaps between the current state and the Standard. Basically, the site privacy and security inspection and the health information registry is done and now the dentists are doing a comprehensive assessment of the practices current practices and systems to see how they compare to the Standard. Again, examples are given that will help the offices understand what is being asked of them. Practices should be able to customize these forms for their particular situation.

3. **Step 3: Develop Privacy and Information Security Policy**: Each dental office must write well-developed and practice specific Privacy and Information Security policies as an essential part of the dentist's ability to comply with the *Health Information Act*. Since these policies are going to be similar for most dental offices in Alberta, the Alberta Dental Association and College has drafted Privacy and Information Security Policies that each practice can customize. This represents **Step 3** and is covered in the **Guide for Developing Information Privacy and Security Practice Specific Policies.**

4. **Step 4: Privacy Impact Assessment:** A Privacy Impact Assessment is an assessment of the custodian's compliance with the *Health Information Act*. The *Health Information Act* anticipates in most cases *that* a Privacy Impact Assessment will be filed by a custodian with the *Office of the Information and Privacy Commissioner of Alberta*. With respect to proposed new collection, use and disclosure of health information a resubmission of the PIA will be required unless the custodian decides that the change is only minor in relation to the policy or protocol previously adopted. It is always prudent if unsure to file an amended Privacy Impact Assessment. This represents **Step 4** and is covered in the **Guide for Preparing Privacy Impact Assessment Submissions and Obtaining Information Manager Agreements**

5. **Step 5: Regularly assess, monitor and update your Privacy Program:** Privacy is not a single event, it an ongoing commitment to our patients that we will protect their privacy and provide appropriate health care.

Resources and Templates Associated with this Guide

1. Templates: Site and Security Inspection, Health Information Registry and Privacy Practice Assessment
2. Guidance for Electronic Health Record Systems – Office of the Information and Privacy Commissioner of Alberta
3. Alberta Dental Association and College: Guide for Patient Records and Informed Consent

B. Developing and Implementing a Practice Privacy Program

1 Introduction and How-to's

The *Health Information Act* (HIA) (Alberta) is privacy legislation that sets out specific rules about the collection, use, disclosure and protection of the health information that dentists, have in their custody and control. Dentists in Alberta are required to comply with *Health Information Act* and in order to do so, it is necessary to go beyond just protecting patient's confidentiality, dentists also need to develop and participate in an ongoing privacy program that addresses accountability, information flow, right of access, and security.

The Alberta Dental Association and College has developed the Standard of Practice: Privacy and Management of Patient Health Information and the Guide for the Alberta *Health Information Act*, which provide a detailed explanation the Act and how it applies to all dentists in Alberta. Before starting, it is necessary to obtain a copy of the *Health Information Act* including the associated regulations. These are available by going to the members' website www.abdentists.com followed by clicking **Health Information Act Resources** under **Quick Links**. Alternatively, they can be found online at www.oipc.ab.ca.

Through use of the Standards, the *Health Information Act* and the Guides, dentists will be able to develop and implement a clear and comprehensive privacy program in their practices.

> ***Quick point:***
>
> The development of practice privacy and security policies for the *Health Information Act* starts here with an outline of the major program areas and the appropriate resources and templates that are included to help address each one.

2 Privacy Officer Role

Each dentist or practice must designate a Privacy Officer who will be responsible for implementing the privacy program using practice-specific policies and any accompanying procedures. The Privacy Officer will be the first and primary contact for all privacy-related inquiries from addressing general questions to processing formal access requests. The Privacy Officer should have sufficient scope of authority and independence and should be as free as possible from conflict of interest situations.

A full description of the Privacy Officer's Roles and Responsibilities should be developed and included with the policies and other documents used to support the practice privacy program. Generally, these will include:

- identifying privacy compliance issues for Practice custodians;
- developing Privacy and Security Policies and procedures;
- reviewing Practice Information Privacy and Security Policies on an annual basis and/or when there are significant changes to *Health Information Act* or other legislation affecting privacy and security at a Practice;
- ensuring that Practice custodians, staff, volunteers and contracted personnel are trained and aware of their duties, roles, and responsibilities under Practice Information Privacy and Security Policy;
- in consultation with Practice Custodians, providing advice on, and interpretation of, applicable privacy legislation, including release/ non-release of information;
- identifying requirements and completing Privacy Impact Assessments (PIA) for Practice programs and health information systems and practices;
- responding to formal requests to practice custodians for access to information, or to correct or amend health information, and facilitating the request process;
- estimating, calculating, invoicing, and approval of waivers of fees relating to request for access to information;
- ensuring the overall security and protection of health information in the custody or control of the Practice;
- directing the practice response to privacy breaches of health information at all practices and facilities in line with policy;
- developing and completing quality assurance processes for implementation of practice privacy program management; and
- representing practice custodians in dealings with third parties, and the Alberta Information and Privacy Commissioner, as necessary.

Quick point:

The Privacy Officer should be identified early in the program development process, should be made aware of the scope of the role and the specific responsibilities and should assist with the self-assessment and policy development.

3 Privacy Program Self-Assessment

The next step in examining the dental practice privacy program surrounding health information involves conducting a self-assessment of the current state of the practice privacy program. This type of assessment can be used to determine which areas of the practice require improvement to better comply with provisions regulating the collection, use, disclosure, retention and destruction of personal health information.

Complete the inspections, reviews and questionnaires. The results of the overall assessment, an evaluation of the current state compared with the expected standards, will help develop a plan to manage the privacy of personal information in the organization.

3.1 Site Privacy and Security Inspection

This is a resource used to conduct an initial walkthrough assessment of the entire practice and to document the current state of privacy practice and protection in each specific area. Start out in the reception or waiting area and work through any practice spaces where personal information (PI) is handled, used, stored, or accessed at any point in time.
Typically, a dental practice could have the following types of spaces:

- Reception/waiting areas
- Administrative work areas
- Treatment rooms
- File storage areas
- Server rooms
- Copy rooms
- Interview areas
- Staff lounge/lunch room
- Hallways/connecting areas
- Off-site workstations (home offices, cars, etc.)

Each area should be identified with a security zone that best fits the use and physical characteristics of the space:

- **Public** –areas that any person can access, including members of the general public, with little to no supervision or restriction. In these spaces, there would be no opportunity to anyone to access practice personal information. This would include a reception or waiting area and any entranceways to these spaces.

- **External** – areas accessed by patients or service providers under sustained supervision or space restriction. Personal information is accessed and used regularly, but only about the specific patient, and under controlled circumstances. Treatment rooms or interview rooms, and connecting hallways, are examples of external zone areas.

- **Internal** – areas generally restricted to staff or authorized persons; patients or external visitors would need to be accompanied and strictly supervised. Personal information

of many patients or employees may be accessed and stored in these spaces, under controlled circumstances. These may be dentists' or administrators' offices, file and storage rooms or areas, reception area workspaces, laboratories, and staff rooms.

- **Restricted** – areas where no patients and only designated staff will have access, under tight restrictions. These areas may contain large volumes of specific kinds of personal information, such as employee files, but could also house system controls and servers, or substances or machinery that may be harmful if not handled safely.

Where each zone ends and a new zone begins, take special note of any physical or even psychological access barriers controlling access from one zone to the next.

Resource information:

When conducting this assessment, identify these areas within the practice and walk through each one, addressing each of the questions, or writing N/A if the questions are clearly not applicable. Take thorough notes about each area – the template can be modified to enlarge the writing space. There will likely have more than 3 areas – the template can be modified to use for additional areas. (ie. print sheet for 4, 5, 6, etc.). Dentists may group some areas together, for instance if all of the treatment rooms are set up exactly the same way, they can be assessed together. There is a space at the end for additional notes.

3.2 Health Information Registry (HIR)

In order to assess and maintain management of the practice's health information to meet health privacy standards, it is necessary to develop and maintain a basic description of what health information the practice has and how it is handled. The Health Information Registry (HIR) provides a standardized, basic description of health information in the practice organized by function.

Collect the information needed for the Health Information Registry as part of the Site Privacy and Security Inspection or from an existing file listing, or as part of dedicated exercise. Below is an explanation of the information needed for each section:

Information Repository

An entry is needed for each "information repository," which is an identifiable grouping of information that has similar functional or content characteristics. These can be a series of case files, a collection of professional or administrative correspondence and transactions organized by subject, a database of financial data, or a scheduling system, regardless the information format.

Function

For each repository, identify which function the information is generated and used to support. Therefore, it is necessary to describe the different functions of the practice in a systematic way. Generally, the functions completed are for which the practice may collect, use, and disclose health information and could include the following:

- Administration
    - Governance, including legal/professional compliance
    - Finances, including billing and insurance claims
    - Marketing/communications
    - Human resources
    - Information management, including privacy management
    - Facilities, supplies and services

- Clinical Operations
    - Scheduling/placement, including referrals
        - Patient care, including:
            - Examination
            - Diagnostics
            - Treatment
            - Dental Hygiene
            - Follow-up
    - Research

Use this functions listing as a guide, but add any other functions that are not covered by these descriptions.

Resource information:

The Alberta Dental Association and College: Guide for Patient Records and Informed Consent is a primary resource. It covers a variety of topic including expected content of patient records, retention requirements, ownership of records, digital communication and electronic recordkeeping systems.

Health Information Elements

This will list the predominant types of health information contained in the information repository. The general categories of health information used in *Health Information Act could be used*:

Registration Information:

- Demographics, including Personal Health Number (PHN)
- Location
- Contact numbers or addresses
- Residency status
- Health information eligibility
- Billing transactions

Diagnostic, treatment and care information

- Health service provided, including professional information about the health service provider

- Donation of body parts or substances
- Medications, health care devices, or equipment provided to and used by patient
- Any other information about the physical or mental health of an individual

Subjects

The general category of individuals the health information documents, such as patients, health providers, employees, contractors, patient family members, etc.

Collection, Use, Disclosure

Identify the purposes for which the health information is collected/used in the practice and for which it is disclosed to external parties. Use the general categories stipulated in *Health Information Act*:

Collection/use/disclosure:

- Providing health services;
- Verifying eligibility to receive a health service;
- Investigations, practice reviews, or inspections of a health professional;
- Research that has been approved by a designated research ethics board;
- To facilitate health service provider education;
- For a purpose authorized by statute; or
- To support internal management, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, processing payments, or human resource management.

Disclosure only

- to government of Canada or another province or territory, for health system management, if:
  - the patient is resident of that region; or
  - that government is paying for the health service;
- to the person providing continuing care of the patient, including family, friends or other non-medical support;
- to family members or close personal friends :
  - if it is limited to presence, location, condition , diagnosis, progress, and prognosis on that day;
  - to contact them if the patient is incapacitated or deceased; or
  - to provide information about circumstances or health service provided surrounding the patient's death; and
  - the disclosure is not against the expressed request of patient;
- to a correctional program officer, for health service or continuing care purposes;
- to a person conducting an audit, if the person agrees in writing:
  - to destroy the information as soon as the audit is completed; and
  - not to disclose the information to anyone other than to report unlawful or improper conduct of a health service provider;
- to a quality assurance committee under Alberta Evidence Act, section 9;
- as part of court or quasi-judicial proceeding to which the custodian is a party;

- to comply with a court order, warrant or subpoena valid within the jurisdiction (mandatory);
- to another custodian, as part of an investigation of fraud, abuse of health services, or to prevent commission of a statutory offence;
- to an officer of the Legislature, for the performance of their duties;
- to avert imminent danger to health or safety of anyone;
- if it is in the best interests of individual who lacks capacity to consent;
- to a descendent of a deceased individual if necessary for the health of the descendant;
- as allowed or required by other laws, in spite of *Health Information Act* provisions;
- to a custodian who is the successor of the dentist 's practice;
- to obtain or process payment for health services by third parties;
- to the College of Physicians and Surgeons of Alberta in compliance with the Triplicate Prescription Program;
- to a health professional body, as part of a complaint or investigation;
- for the purpose of assessment and storage at a public body archives; or
- for registration information only, to collect or process a debt or fine owing.

Security/Location

Describe the locations where the information is stored, used, accessed, included off-site locations and electronic networks. Describe the security measures used to mitigate risk of unauthorized access, loss, or revision of information.

Resource information:

The Guidance for Electronic Health Record Systems – Office of the Information and Privacy Commissioner of Alberta provides an understanding of the requirements under the *Health Information Act* for practice management systems including such technology as digital radiography and 3-D imaging including cad-cam, cone-beam and digital impression technology. In addition, it covers many of the elements that will be identified during as the *Site and Security inspection, Health Information Registry and Privacy Practice Assessment template gathering process*.

Retention

State how long the information is retained, either active or in inactive, and when it is destroyed.

Privacy Impact Assessment (PIA) Needed?

1. Identify whether there is an existing Privacy Impact Assessment that covers this repository or whether a Privacy Impact Assessment is needed based on the criteria in the practice Privacy Impact Assessment policy. A Privacy Impact Assessment is an assessment of the custodian's compliance with the *Health Information Act*. The *Health Information Act* anticipates in most cases that a Privacy Impact Assessment will be filed by a custodian with the Office of the Information and Privacy Commissioner of Alberta. With respect to proposed new collection, use and disclosure of health information a resubmission of the PIA will be required unless the

custodian decides that the change is only minor in relation to the policy or protocol previously adopted. It is always prudent if unsure to file an amended Privacy Impact Assessment. A custodian must prepare a Privacy Impact Assessment and must submit it to the Alberta *Office of the Information and Privacy Commissioner* prior to implementing the change in practice or system. This represents **Step 4** and is covered in the **Guide for Preparing Privacy Impact Assessment Submissions and Obtaining Information Manager Agreements.** For more information on Privacy Impact Assessments see the Alberta *Office of the Information and Privacy Commissioner* website www.oipc.ab.ca

Resource information:

The forms have been populated with text for each section illustrating how the registry would be completed. Customization based on the actual circumstances in a dental practice is required.

3.3 Practice Privacy Assessment

This resourcel provides the core, comprehensive assessment of the practice's current privacy practices and systems. Part 1 deals with the practice as whole. Part 2 will be completed for each function in the practice. The completed Health Information Registry for the practice will identify these functions. The functions operating in the practice may include the following:

- Administration
  - Governance, including legal/professional compliance
  - Finances, including billing and insurance claims
  - Marketing/communications
  - Human resources
  - Information management, including privacy management
  - Facilities, supplies and services

- Clinical Operations
  - Scheduling/placement, including referrals
  - Patient care, including:
    - Examination
    - Diagnostics
    - Treatment
    - Dental Hygiene
    - Follow-up
  - Research

The assessment resource is organized in sections comprising the main components of a standard privacy program:

- Practice Privacy Program Organization Management
- Limited Collection and Use Practices
- Limited Disclosure and Consent Practices

- Individual Access to Information
- Security and Information Management to Protect Privacy

Within each section are a series of entries describing the required privacy standards. Identify how and how well the practice currently meets this standard and, if there are significant gaps between the current state and the standard, what actions have or will be taken to close the gap.

Quick point:

By identifying the gaps that exist between the current state and the requirements of the *Health Information Act* dentists have a basis to take action to meet their obligations.

4 Privacy and Information Security Policies

Written well-developed and practice-specific policies are an essential part of the practice's ability to comply with *Health Information Act*. The practice privacy policies inform both staff and members of the public that privacy is recognized and respected by the organization.

Business practices aimed at protecting personal health information include specific components of a privacy policy with directives as to how the organization will collect, use and disclose personal information and how personal information will be managed, including use of records retention and destruction schedules.

The practice policies must also include steps for informal and formal requests for access and correction to personal information and indicate to whom requests are to be forwarded. The policies provide direction on the kinds of records that may be available outside the legislation and what records might constitute an unreasonable invasion of privacy if disclosed without consent.

Privacy policies provide an established direction for everyone in the practice and the practice's patients on questions concerning consent for collection, use and disclosure of personal information, how personal information is to be managed, maintained securely, stored and the steps to be followed in the event of a breach of personal information. Polices must be reviewed and updated regularly.

The **Guide for Developing Information Privacy and Security Practice Specific Policies, which is Step 3,** outlines the development of the policies. It includes template documents that can be used to assemble a complete set of policies consistent with the *Health Information Act*. This sample set of policies is based on recommendations included in the Alberta Dental Association and College Standards, the Office of the Information and Privacy Commissioner of Alberta: Privacy Impact Assessment Requirements and the *Health Information Act*. Each section in the **Guide for Developing Information Privacy and Security Practice Specific Policies** is preceded by an explanation of the reason for the policy and a description of what should be included in the policies the practice develops.

Resource information:

Remember these are examples only, the dental practice must use the information gathered while using the **Guide for Implementing the Requirements of the *Health Information Act*** to help evaluate the sample policies, and consider how they will be customized to fit the individual practice. Dentists may decide to structure the policies any way they want, as long as the essential content is included.

4.1 Training Resources

Staff training is an important aspect of compliance with privacy legislation. Training will be based on the information in the Alberta Dental Association and College Standards, the accompanying Video Modules and the policies and procedures developed to support the practice privacy program. The Video Modules were previously identified during **Step 1** as resources for the Guide **for the Alberta Health Information Act: Privacy and Management of Patient Health Information.** They like all information related to the *Health Information Act* can be located by going to the members' website www.abdentists.com followed by clicking **Health Information Act Resources** under **Quick Links.** The Staff needs to understand the importance of and value of personal health information, why it needs to be collected properly, protected from unauthorized collection, use, disclosure or destruction and what the repercussions are for improper practices. In larger practices, it may be helpful to consider different levels of training for designated groups within the organization. For example, administrators and other support staff may not require the same level of training, as would dental assistants who work with personal health information on a day-to-day basis. Training can be facilitated by the dentist, the Privacy Officer, or by an independent expert facilitator. New employees should receive training prior to the start of their jobs. Existing employees should receive regular training and special sessions when and if there are significant changes in the practice or in the legislation that affect the practice privacy program. Practices should track when training occurs and who attends.

Quick point:

Keeping track of training provided and who attends is an important component of a privacy program.

Resource information:

The following sample forms for Site and Security Inspection, Health Information Registry and Privacy Practice Assessment are provided as a resource template associated with this Guide. This template is titled **Site and Security Inspection, Health Information Registry and Privacy Practice Assessment Template**.

C. Site Privacy and Security Inspection – (example)

Practice Name:	*Location:*	*Inspection completed by:*	*Date:*

INSPECTION QUESTIONS	Area A: Reception/Waiting Area	Area B: Treatment Rooms	Area C: Administration Area
	X *Public* *External* *Internal* *Restricted*	*Public* X *External* *Internal* *Restricted*	*Public* *External* X *Internal* *Restricted*
1. Previous assessments Have there been previous security assessments of the business unit?	Informal only	Informal only	Informal only
2. Verbal confidentiality Can unauthorized persons hear verbal exchange of PI?	Yes. -Reception/waiting area close. -Conversations can be heard by patients waiting	Yes. -No doors -Divider walls open between treatment rooms	No. -Door able to be closed -Out of heavy traffic area
3. Visual confidentiality Can unauthorized persons see computer or device monitors? Are monitors turned away or covered by privacy screens? Are PI records covered, put away or supervised at all times? Do screens time-out if unattended?	No. -Monitors are turned away from public -Monitors time out when not in use -Patient information program is password protected -No ability to close-off or lock paper records during non-business hours	Yes. -Monitors not always turned away from patient view -Monitors time out when not in use	No. -Computer screen not legible unless office is entered -Monitor times out when not in use -Records are supervised during business hours -Records are put away in filing cabinet -Door to admin office not locked during non-business hours – staff need access to fax machine

INSPECTION QUESTIONS	Area A: Reception/Waiting Area	Area B: Treatment Rooms	Area C: Administration Area
4. Video surveillance Is the area under video surveillance? Is there a notification that the areas is under surveillance? Are surveillance tapes securelystored? How long are they retained?	No.	No.	No.
5. Access Barriers Are locks or barriers secure? If no locks, are area entrances supervised at all times? Authentication level for entry to areas or devices? 1. Knowledge (password) 2. Possession (key fob) 3. Inherent (biometrics) Is distribution of area access keys or codes managed? Are both authorized persons and guests identified? Is the area alarmed? Are devices or computers logged out when unattended, requiring authentication to log in?	-Building is armed during non-business hours -Computers are shut down during non-business hours except for server which is logged out -Password is required to access patient information system -area is supervised during business hours -Access door to area is locked during non- business hours	-Building is armed during non-business hours -Computers are shutdown during non-business hours -Area is supervised during business hours -Main door to area is locked during non- business hours -Computers are not password protected	-Building is armed during non-business hours -Computer is shutdown during non-business hours -Computer is password protected -Door to office is closed but not locked during non-business hours -Area is supervised during business hours -Main door to area is locked during non- business hours
6. PI storage Are there overnight locked rooms or cabinets for Files Servers Computers containing PI Is PI in garbage/recycling bins secured? Are networked PI directories segregated or secured?	-Door to patient file area is locked during non-business hours -File shelves have no locking ability -Computers are password protected -Patient information recycling kept in reception area (not secure) until put in locked bin	-No patient information garbage -Sometimes patient charts are left in the treatment lab area	-Door to area closed but not locked -Filing cabinets not locked -Computer is password protected -Patient information garbage is shredded

INSPECTION QUESTIONS	Area A: Reception/Waiting Area	Area B: Treatment Rooms	Area C: Administration Area
7. Safety Heat/smoke alarms? Sprinklers? Non-water suppressants?	-Smoke alarm located outside elevator -Access for fire extinguishers -No sprinkler system	-Smoke alarm located outside elevator -Access for fire extinguishers -No sprinkler system	-Smoke alarm located outside elevator -Access for fire extinguishers -No sprinkler system
8. Mail/Courier Is mail or courier service reputable and secure? Is PI placed in sealed envelopes? Does staff avoid large aggregations of PI?	-Canada Post, Purolator, DHL, Greyhound -Always receive sealed package/envelope -Outgoing items always sent in sealed package/envelope -Only necessary patient information is collected	N/A	-All incoming and outgoing mail is sealed
9. Electronic Transmission Is electronic PI transmitted over dedicated lines or channels? Is PI encrypted when transmitted through public networks or providers? Is transmission logged and monitored?	-Insurance claims submitted via EDI through CDANet -Some referrals are send to specialists on- line (No indications as to "entering a secure site")	N/A	N/A
10. Fax/Printer Transmission Is access to networked printers controlled? Are fax machines and printers located in secure, non-public areas? Are cover sheets used for every fax transmission of PI Are recipient of PI stored as speed dial entries Is receipt of PI confirmed?	-Fax machine located in admin office -Cover sheets are used with every outgoing fax -No speed dial -No confirmation of receipt -All printers located in supervised areas	N/A	-Fax machine located in admin office -Cover sheets are used with every outgoing fax -No speed dial -No confirmation of receipt

ADDITIONAL NOTES:

Practice Name:	*Location:*	*Inspection completed by:*	*Date:*

INSPECTION QUESTIONS	**Area D: Hallways**	**Area E: Staff Lounge**	**Area F: Dead Filing**
	☐ *Public* ☒ *External* ☐ *Internal* ☐ *Restricted*	☐ *Public* ☐ *External* ☒ *Internal* ☐ *Restricted*	☐ *Public* ☐ *External* ☒ *Internal* ☐ *Restricted*
1. Previous assessments Have there been previous security assessments of the business unit?	Informal only	Informal only	Informal only
2. Verbal confidentiality Can unauthorized persons hear verbal exchange of PI?	Yes. -No doors on treatment rooms	No. -Located in the basement -Door closed at all times	No. -Located in the basement -Door closed at all times
3. Visual confidentiality Can unauthorized persons see computer or device monitors? Are monitors turned away or covered by privacy screens? Are PI records covered, put away or supervised at all times? Do screens time-out if unattended?	Yes. -Treatment rooms are open to the hallways -Computer at end of hall can be seen -Monitor times out when not in use	No. -No computers or paper records are located here	No. -No computers -Door is always closed but not locked

INSPECTION QUESTIONS	Area D: Hallways	Area E: Staff Lounge	Area F: Dead Filing
4. Video surveillance Is the area under video surveillance? Is there a notification that the areas is under surveillance? Are surveillance tapes securely stored? How long are they retained?	No	No	No
5. Access Barriers Are locks or barriers secure? If no locks, are area entrances supervised at all times? Authentication level for entry to areas or devices? 1. Knowledge (password) 2. Possession (key fob) 3. Inherent (biometrics) Is distribution of area access keys or codes managed? Are both authorized persons and guests identified? Is the area alarmed? Are devices or computers logged out when unattended, requiring authentication to log in?	-Building is armed during non-business hours -Main doors to area locked during non-business hours -Area is supervised during business hours -Computer shutdown during non-business hours -No password protection	-Building is armed during non-business hours -Main door to area locked during non-business hours	-Building is armed during non-business hours -Door to area closed but not locked -Main door to area locking during non- business hours -No computer
6. PI storage Are there overnight locked rooms or cabinets for Files Servers Computers containing PI Is PI in garbage/recycling bins secured? Are networked PI directories segregated or secured?	-No patient information garbage -Occasionally patient charts are left in area (by computer)	-No patient information garbage -No computers	-Patient charts with no new entries for 10 years are pulled and reviewed to determine if they can be formally disposed * Policy required that sets out formal retention and disposition schedule and protocols for health and personal information

INSPECTION QUESTIONS	Area D: Hallways	Area E: Staff Lounge	Area F: Dead Filing
7. Safety Heat/smoke alarms? Sprinklers? Non-water suppressants?	-Smoke alarm located outside elevator -Access to fire extinguishers -No sprinkler system	-Smoke alarm located outside elevator -Heat/cold alarm in furnace room -Access to fire extinguishers -No sprinkler system	-Smoke alarm located outside elevator -Heat/cold alarm in furnace room -Access to fire extinguishers -No sprinkler system
8. Mail/Courier Is mail or courier service reputable and secure? Is PI placed in sealed envelopes? Does staff avoid large aggregations of PI?	N/A	N/A	N/A
9. Electronic Transmission Is electronic PI transmitted over dedicated lines or channels? Is PI encrypted when transmitted through public networks or providers? Is transmission logged and monitored?	N/A	N/A	N/A
10. Fax/Printer Transmission Is access to networked printers controlled? Are fax machines and printers located in secure, non-public areas? Are cover sheets used for every fax transmission of PI Are recipient of PI stored as speed dial entries Is receipt of PI confirmed?	-Printers located in supervised areas	N/A	N/A

ADDITIONAL NOTES:

Practice Name:	*Location:*	*Inspection completed by:*	*Date:*

INSPECTION QUESTIONS	**Area G: Consult Room**	**Area**	**Area**
	[ ] *Public* [X] *External* [ ] *Internal* [ ] *Restricted*	[ ] *Public* [ ] *External* [ ] *Internal* [ ] *Restricted*	[ ] *Public* [ ] *External* [ ] *Internal* [ ] *Restricted*
1. Previous assessments Have there been previous security assessments of the business unit?	Informal only		
2. Verbal confidentiality Can unauthorized persons hear verbal exchange of PI?	No. -Pocket door can be closed		
3. Visual confidentiality Can unauthorized persons see computer or device monitors? Are monitors turned away or covered by privacy screens? Are PI records covered, put away or supervised at all times? Do screens time-out if unattended?	Yes. -People walking down hallway can look in -Door usually not closed -Monitor times out when not in use		

INSPECTION QUESTIONS	Area G: Consult Room	Area	Area
4. Video surveillance Is the area under video surveillance? Is there a notification that the areas is under surveillance? Are surveillance tapes securely stored? How long are they retained?	No		
5. Access Barriers Are locks or barriers secure? If no locks, are area entrances supervised at all times? Authentication level for entry to areas or devices? 1. Knowledge (password) 2. Possession (key fob) 3. Inherent (biometrics) Is distribution of area access keys or codes managed? Are both authorized persons and guests identified? Is the area alarmed? Are devices or computers logged out when unattended, requiring authentication to log in?	-Building is armed during non-business hours -Area is supervised during business hours -Main doors to area are locked during non-business hours -Computer is shutdown during non- business hours -No password protection		
6. PI storage Are there overnight locked rooms or cabinets for Files Servers Computers containing PI Is PI in garbage/recycling bins secured? Are networked PI directories segregated or secured?	-No patient information garbage -Occasionally patient charts are left in the area		

INSPECTION QUESTIONS	Area G: Consult Room	Area	Area
7. Safety Heat/smoke alarms? Sprinklers? Non-water suppressants?	-Smoke alarm located outside elevator -Access to fire extinguishers -No sprinkler system		
8. Mail/Courier Is mail or courier service reputable and secure? Is PI placed in sealed envelopes? Does staff avoid large aggregations of PI?	N/A		
9. Electronic Transmission Is electronic PI transmitted over dedicated lines or channels? Is PI encrypted when transmitted through public networks or providers? Is transmission logged and monitored?	N/A		
10. Fax/Printer Transmission Is access to networked printers controlled? Are fax machines and printers located in secure, non-public areas? Are cover sheets used for every fax transmission of PI Are recipient of PI stored as speed dial entries Is receipt of PI confirmed?	-Printers located in supervised areas		

D. Health Information Registry – (example)

Practice Name:	*Date:*

PART 1 HEALTH INFORMATION DESCRIPTION				PART 2 INFORMATION FLOW		PART 3 INFORMATION MANAGEMENT		
#	Information Repository	Function	Health Information Elements	Subjects	Collection, Use, Disclosure	Security/Location	Retention	PIA Needed?
1	Patient Files (active)	Patient Care - *Examination* - *Diagnostics* - *Treatment* - *Dental Hygiene* - *Follow-up*	Patient contact, medical status, diagnostic, treatment, care, billing, insurance information, health alerts, medications, additional patient and account notes	Practice patients	-Collect/use to support patient health services, determine eligibility for services, and to process payment for services -Disclosure to laboratories, dental service providers, specialists to support patient health services, determine eligibility for services, -Disclosure of services to insurance companies and other third party payers to process payment for services	**Active files**: in shelves behind reception workstation, supervised during business hours, area locked at night. Used in reception workstation, paper copy only in examination rooms, and may be taken off-site. Computer access to patient information system by reception workstations. Each workstation is password protected. **Inactive Files**: Stored on shelves in basement.	Patient records for adults remain accessible for a minimum period of ten (10) years following the date of last service, and patient records for minors are accessible for a minimum period of ten (10) years past the patient's age of majority. In the event of a patient becoming deceased, the retention period is not changed.	In most cases, a PIA will be required to be filed with the OIPC as part of this review unless there is a previously submitted PIA.
2	Practice Billing System (Patient)	Finances	Patient contact, dental services performed, billing, insurance information, additional patient and account notes	Practice patients	-Collect/use to process payment for services -Disclosure of services to insurance companies and other third party payers to process payment for services	Access by reception workstations using password protection. Supervised during business hours. Automated transmission of claims to 3rd party insurance using CDANet.	Same retention period as number 1	Same as 1

PART 1 HEALTH INFORMATION DESCRIPTION				PART 2 INFORMATION FLOW		PART 3 INFORMATION MANAGEMENT		
#	Information Repository	Function	Health Information Elements	Subjects	Collection, Use, Disclosure	Security/Location	Retention	PIA Needed?
3	Scheduler	Patient Appointments	Patient contact, booked appointments, recalls, planned and future treatments	Practice patients	-Collect/use to produce daily work schedules. -Disclosure to other service providers or specialists when coordination of appointments is necessary.	Access by reception workstation using password protection. Supervised during business hours.	7 calendar years	Same as 1
4	Digital Xray and Photographs	Patient xrays, photos, treatment	Patient name and address, xrays & photos taken by our office or received from other offices.	Practice patients	-Collect/use for diagnostic purposes, verification of dental services provided, treatment planning. -Disclosure to other health/dental service providers & specialists to support patient dental health services.	Access by receptionists, treatment rooms and consult room (no password protection). Areas supervised during business hours Forward to other service providers via encrypted email or courier, mail Canada Post in sealed package.	Same retention period as number 1	Same as 1
5	Patient Models & Lab Cases	Patient treatment	Patient name, diagnostic treatment, care	Practice patients	-Collect/use for diagnostic and treatment planning -Disclosure to labs for fabrication of crowns, bridges & appliances	Active treatment cases stored in treatment lab area. Supervised during business hours. Main door to area locked during non-business hours. Deliver to lab either in person (to lab in basement) or by courier in sealed package. Finished cases stored in basement in marked bins. Door to area closed but not locked	Same retention period as number 1	Same as 1

PART 1 HEALTH INFORMATION DESCRIPTION				PART 2 INFORMATION FLOW		PART 3 INFORMATION MANAGEMENT		
#	Information Repository	Function	Health Information Elements	Subjects	Collection, Use, Disclosure	Security/Location	Retention	PIA Needed?
6	Human Resources (staff files)	Staff information	Staff contact, SIN, salary information, date of birth, hire date, payment information, hours of work	Practice staff	-Collect/use for payment of salary and human resource management. -Disclosure to Government in the form of T4's, and to owners to sign payroll cheques.	Access by Office Manager workstation – password protected. Area supervised during business hours. Door to office closed during non-business hours. Main door to area locked during non-business hours.	HR Information back to 1992	Same as 1
7	Payables (vendor)	Vendor/Payables information	Vendor contact and payments	Suppliers	-Collect/use for payment to suppliers and G/L management. -Disclosure to owners to sign cheques & to accountant for year-end purposes	SAME AS ABOVE	7 years	Same as 1
8	Patient Files (inactive)	SAME AS ACTIVE	SAME AS ACTIVE	Practice patients	Inactive files pulled if patients return to practice for treatment.	Stored on shelves in basement storage room. Door to room closed but not locked	Same retention period as number 1	Same as 1

E. Practice Privacy Assessment – (example)

Practice Name:	*Assessor:*	*Date:*
Custodians Participating:		

Privacy Standard/Questionnaire		Current State	Action/Status
PART 1: PRACTICE PRIVACY PROGRAM ORGANIZATION AND MANAGEMENT *Complete for each clinic or practice*			
Practice leadership plans, designs, and management structures for privacy compliance set clear and consistent expectations and policy, assign accountabilities effectively, and provides adequate resources to support compliance. *Risk:* *When privacy management processes, structures, responsibilities and time and resources are inadequate, unclear, ill-informed, constrained, inaccessible, arbitrary, or inconsistent, the function will not be able to comply with practice privacy policies.*			
1 POLICY AND PROCESS			
1.1	Privacy policies provide clear and specific enough direction for the Practice staff in this function.		- Design policy to provide clear and specific direction
1.2	All staff are able to identify privacy risks and respond to access requests, complaints, and breaches in the appropriate way based on policies and process standards.		- Will be described in policy

Privacy Standard/Questionnaire		Current State	Action/Status
1.3	There is a process in place to assess, train, monitor, and decommission contractors in the function providing services involving health information in line with practice privacy compliance standards.	- The only contract-type we have are janitorial staff and building maintenance - painter	- N/A at this time
1.4	Adherence to privacy and security standards are in clearly established as conditions of employment.	- Privacy is discussed when hiring new staff.	- New and existing still have be required to read the Privacy Policy and sign Confidentiality Oath
2 ACCOUNTABILITY			
2.1	Staff in this function know who the Privacy Officer is and when and how to get this person involved when handling health information according to assigned responsibilities.	- Current Privacy Officer – Dr. ????	- Dentist to be the Privacy Officer - Business Manager to be Privacy Coordinator - When & how to involve the Privacy Officer will be specified in the policy
2.2	Privacy expectations for third party contractors handling or accessing health information are included in the contractual terms of outsourcing or service agreements.	- Contractor privacy agreement in place and signed by janitorial and maintenance staff (sample attached)	
2.3	Contracts and service agreements with the Practice are reviewed for consistency with practice privacy policies and regulatory requirements.	- Never amended or changed	- Review annually

Privacy Standard/Questionnaire		Current State	Action/Status
2.4	Practice knows what health information is under its custody and control and how it is being managed and protected, including information managed by third party contractors.		OK
2.5	Function personnel can answer privacy related questions fully and in a timely manner when asked by individuals.		OK
2.6	There are sanctions in place for violation of privacy policy, and Practice staff are made aware of them.		- Staff to read and sign Confidentiality Oath
3 COMMUNICATION AND RESOURCES			
3.1	There are printed, published, or on-line materials and forms to adequately support privacy practices in this function.		- Will add information to our new website (Post complete policy?)
3. 2	Management allocates adequate resources and time to privacy compliance sufficient to meet the demands of the function.		- Review annually or as needed

Privacy Standard/Questionnaire		Current State	Action/Status
3.3	All staff with accountabilities are knowledgeable and effectively trained to implement privacy compliance standards in a timely way.		- Staff to be trained upon employment
3.4	Function staff are appropriately screened and monitored to establish their ability to meet privacy and security standards.		- Screened upon employment
3.5	There is information about the health information held by the function available to both the staff and individuals that describes how and for what purpose and authority the health information is collected, used, disclosed, retained and protected.	- Patient Privacy Consent form in place (see attached)	OK
4 REVIEW AND CHANGE			
4.1	Changes in accountability roles and responsibilities and personnel are completed effectively and quickly, with little loss in service.		OK. We have enough staff to cover until new employees are trained
4.2	Changes in legislation, regulation and best practices are tracked, assessed and applied to management policy.		- Changes to policy to be done as required.

Privacy Standard/Questionnaire		Current State	Action/Status
4.3	There is a periodic review of health information collection, use, disclosure, retention and security practices both within the function and with contractors to identify practices and changes that may affect privacy compliance.		- Review Annually - Complete initial PIA and file with Office of Information and Privacy Commissioner
4.4	When the function identifies changed conditions, practices, IT systems, and processes that may affect privacy in the function and with contractors, a Privacy Impact Assessment is completed before the change occurs and without unduly delaying required change.		- Complete PIA before implementation of new practices, IT system or process
4.5	There is a process for review of relevant forms, materials, and to ensure that they are accurate and up to date and that obsolete versions are deleted from use.		- Review Annually

Practice Name:	*Assessor:*	*Date:*
Custodians Participating:		

Privacy Standard		Current State	Action/Status
PART 2: FUNCTION PRIVACY REVIEW *Complete for each function in the clinic or practice*			
1. LIMITED COLLECTION AND USE PRACTICES **Function collects and uses only the amount of health information reasonably required to fulfill its operational requirements and consistent collection and use authorities and notice procedures.** ***Risk:*** ***If too much health information is collected and used for unauthorized purposes:*** ***1. The individual is harmed by possible application of their health information beyond what they had wanted or is in their best interest*** ***2. More health information is unnecessarily to possible privacy breaches*** ***3. The Practice is exposed to an increased number or complaints and questions about collection for legitimate purposes***			
1.1	Function can identify and rationalize collection and use of health information based on policy of collecting the least amount of health information required for reasonable health or operational purposes.	- Patient Health Questionnaire - Patient Information screen in Power Practice	*Office needs to develop formal policy
1.2	There are criteria and processes to ensure that staff collects health information indirectly from someone other than the individual only for purposes allowed by policy or law.	** Do we need both 1.2 & 1.3?	Same as 1.1

Privacy Standard		Current State	Action/Status
1.3	Personal information collected from sources other than the individual is reliable and has been obtained by the source by fair and lawful means.	- Collection of personal information from parent/guardian or representative	Same as 1.1
1.4	When consent is required, health information is collected directly from the individual or their authorized representatives and only after the individual has consented in the proper form.	- The HIA is legislation that does not contemplate the need for written consent. Instead the "express wish" of patient in some circumstances may need to be considered	Same as 1.1
1.5	Processes are in place to ensure that the health information collected and used is complete and accurate.	- Information collected as per Patient Information screen in Practice X	Same as 1.1
1.6	There is a periodic review of health information collection and use to ensure that it is still limited to what is needed for legislative and operational purposes.	- Medical histories reviewed yearly - Confirmation of contact information (phone #, etc) when appointments are booked - Insurance Information as presented	Same as 1.1
1.7	Individuals are notified before collection of health information, and notices are clear, conspicuous, and effective.	- Personal Information consent form in place. - PI consisting of DOB, address, phone # collected before new patient appointment is booked	Same as 1.1
1.8	Notices to individuals from whom health information is collected include at minimum:	- Personal information consent form in place	- Same as 1.1 - Post "Your Health Information at our Clinic" poster

Privacy Standard		Current State	Action/Status
1.8.1	A description of the health information collected and used;	- Personal information consent form in place	- Same as 1.1 - Post "Your Health Information at our Clinic" poster
1.8.2	Purpose and authority for which the health information is being collected, used or disclosed;	- Personal Information consent form in place	- Same as 1.1 - Post "Your Health Information at our Clinic" poster
1.8.3	A reference to the practice privacy policy and Privacy Officer should the individual require further information.		- Information to be added to our new website (Post complete policy?) - Add website to "Your Health Information at our Clinic" poster
1.9	Function uses passive (e.g., poster or pamphlet), active (e.g., telling the individual before asking), written or verbal notices appropriate to the sensitivity of the health information or the purpose.		- Post "Your Health Information at our Clinic" poster
1.10	Staffs know that only staff members with a functional need relating to the specific patient can access health information of a patient.	- Both clinical and receptionist staff have access to patient charts	Same as 1.1

Privacy Standard		Current State	Action/Status
2. LIMITED DISCLOSURE AND CONSENT PRACTICES **Function discloses health information they hold about patients for authorized health purposes and/or in line with relevant consents and notices.** ***Risk: If health information is disclosed for unauthorized purposes to outside organization without the consent of the individual:*** ***1. The interests of individuals are harmed by inappropriate application of their health information by other persons or organizations out of their control;*** ***2. The Practice will lose credibility and trust of its patients.***			
2.1	Function limits disclosure of health information they hold or based on purposes consistent with notices and consents provided by the individual or in accordance with policy and law.		- Specify limitations in policy
2.2	Processes and criteria are in place to ensure that only staff that have a need to know based on operational and functional need related to their position are given access to health information.	- Clinical & reception staff have access to patient charts	OK
2.3	Personal information is retained only for as long as reasonably required for identified business purposes.	- Paper charts kept for 10 years	OK
2.4	A process is in place to update and validate health information, when needed to support the purpose for which it is collected, used and disclosed.	- Medical history updated yearly - Contact information confirmed upon appointment booking	OK

Privacy Standard		Current State	Action/Status
2.5	The function can identify what information has been disclosed to third parties, and for what purpose.	- Notes written in paper chart	OK
	There is a process and mechanism in place to allow patients to request that all or part of their health information not be disclosed, and, if considered reasonable, that this request can be implemented either manually or electronically.	- Release of records consent form in place (see attached)	OK
2.6	Function staff knows when consent is needed by policy and law.		- Specify in Policy
2.7	Consents for disclosure of health information include at minimum:	- Patient release of records consent form used when sending info to a new dentist requested by patient	- Could use Consent for Disclosure of Patient Information form
2.7.1	An authorization to disclose specific health information described;		- Use Consent for Disclosure of Patient Information form
2.7.2	The identity of the persons or organization to whom the health information will be disclosed;	- Referral to specialists or other dentists for treatment. - As requested by other healthcare providers or insurance companies (Sent without consent) - Disclosure is noted in chart	OK

Privacy Standard		Current State	Action/Status
2.7.3	Purpose and authority for which the health information will be disclosed;	- For dental/health care - Disclosure is noted in chart	OK
2.7.4	An acknowledgement that the subject understands fully the risks and benefits of the disclosure, or refusing to consent.	- Do not think we have run into a situation where a patient would not consent.	- Makes notes in chart if patient refuses to consent to disclosure
2.7.5	Dates when consent is effective, if required by subject		- Use Consent for Disclosure of Patient Information form
2.7.6	Statement that the consent can be revoked at any time.		- Use Consent for Disclosure of Patient Information form
2.8	There is an accessible and effective process to accommodate and document when an individual changes or withdraws consent.		- Make documentation on Consent for Disclosure of Patient Information Form
2.9	Consent is obtained when health information disclosed by consent is disclosed for any new purpose.		- Use new Consent for Disclosure in Patient Information form

Privacy Standard		Current State	Action/Status
2.10	There is a confirmation process to ensure that the person consenting is authorized to make the consent for the individual whose health information is being collected, used, or disclosed.		- If possible get a copy of the Enduring Power of Attorney or any other documentation specifying authorization
3. INDIVIDUAL ACCESS TO INFORMATION **Function provides individuals with comprehensive and timely access to and review of their own health information, in compliance with policy and law** ***Risk:*** ***If processes for facilitation access and review to information by individuals are incomplete, lengthy, inconsistency and result in:*** ***1. Individuals' inability to effectively determine of the collection, use, and disclosure of their health information in the Practice;*** ***2. The practice is in danger of violating an individual right established in privacy law;*** ***3. Individual requests for review and complaints to the regulator are more likely to increase.***			
3.1	Function know and effectively makes timely and appropriate use of the routine or formal process for responding to requests for access and correction of a patients' own health information.	- Change in contact and insurance information done as required	OK
3.2	If a formal request is required, individuals are effectively informed about how to make a request for access or correction of their health information, when this process is appropriate.		- Describe in policy
3.3	The requesting individual's identity is confirmed before access is granted.	- Usually not needed as patients are known	- Include in Policy

Privacy Standard		Current State	Action/Status
3.4	Granting of access does not disclose any other individual's health information.		OK
3.5	Function staff know and use the appropriate process for the individual to correct or to register disagreement with the accuracy of the health information retained.	???	
4. SECURITY AND INFORMATION MANAGEMENT TO PROTECT PRIVACY **Functions implements and maintains effective measures to prevent unauthorized internal and external access to, loss, or manipulation of health information they hold.** ***Risk:*** ***If health information is poorly protected in the function:*** ***1. The Practice increases its exposure to privacy breaches beyond what is acceptable;*** ***2. Individuals whose health information is breached can be directly harmed;*** ***3. The practice may lose credibility and trust of its employees and patients.*** ***For sections 4.1-4.9, use the information compiled in the Site Privacy and Security Inspection Form**			
4.1	Verbal exchanges of health information are out of hearing from unauthorized persons.	- Waiting areas are close to reception area – unauthorized persons could overhear conversations	- Keep voices down to alleviate unauthorized people hearing conversations

Privacy Standard		Current State	Action/Status
4.2	Unauthorized persons are not able to view health information of others inadvertently or with little effort, and health information is either locked away or supervised at all times.	- Reception area is supervised at all times during business hours, computers are not visible - Treatment area computers are visible	- Have the current patient's information displayed on screens in clinical area - Minimize when not in use
4.3	Video surveillance is used for reasonable security reasons and patients and employees are notified.	NO	
4.4	There are physical, supervisory, and electronic access barriers are in place between different security zones, and distribution and use of access keys, IDs, passwords and access devices is controlled and secured by staff.	NO	
4.5	Areas and systems where health information is stored on site are physically or electronically restricted to ensure only those authorized can access the information.	- Reception workstations are password protected. - Treatment area workstations are not password protected. - Main doors leading to areas are locked during non-business hours.	- Password protect workstations in treatment area
4.6	There are adequate fire alarms and suppressant systems in place to protect information from fire damage.	- Fire alarms and access to fire extinguishers	OK
4.7	Personal information sent by mail and courier services is adequately secured from loss or unauthorized access during transport.	- Sent in sealed envelope or package	OK

Privacy Standard		Current State	Action/Status
4.8	Personal information transmitted electronically over public transmission networks (internet or phone) is secured from external interception.	- Insurance claims send over CDANet - Confirmed with Practice X that information sent is encrypted	OK
4.9	Fax, printer and e-mail transmissions are used and prepared to ensure that health information is received securely by the intended recipient only.	- Fax transmission sheets used for every outgoing fax contains a Confidentiality clause on the bottom (see attached)	- Add "Confidentiality" footer to outgoing emails
4.10	Function staff know the processes in place to effectively identify and respond to privacy breaches, or unauthorized attempts to access health information.		- Add information to Policy
4.11	There are processes and resources in place to securely and completely dispose of health information in both paper and electronic form.	- Paper charts shredded on-site - Electronic information kept	Describe in policy
4.12	Audit logs are in place to document access by authorized users to health information in electronic systems, including: • Name of user and role • Date/time of access • Actions performed on record • Workstation used • Name/ID of patient		** Need to check with Practice X

Privacy Standard		Current State	Action/Status
4.13	Processes are in place and implemented to determine who are the authorized users, grant access privileges and permissions and maintain the access permissions as current authorized users based on functions.		- All staff, clinical and reception have access to complete patient information - Practice X access only from reception area. - Patterson Imaging access in treatment rooms and reception
4.14	Personal information is retained and destroyed according to a set schedule.	- Inactive files are purged regularly and destroyed on-site "Shred-It"	OK
4.15	When health information in both paper and electronic form is destroyed, there is a process in place to ensure that the destruction was carried out securely and completely	- Inactive files are purged regularly and destroyed on-site "Shred-It" - Electronic files not destroyed	OK
4.16	Remote electronic access to function health information is over secured transmission and in circumstances that meet the standards of on-site security	- No remote access to personal health information - Firewall hardware device running DDWRT linux firewall services. The only open inbound ports are to enable receiving of incoming email messages. All other inbound ports are blocked.	OK
4.17	There is periodic testing of logical and physical security processes to ensure their effectiveness.	- Bi-annual update to logical security devices firmware and software. - User station security patches and threat definitions are automatically applied.	OK

Privacy Standard		Current State	Action/Status
4.18	Function systems that hold critical or sensitive information are backed up on a daily basis and are stored in a secure off-site environment.	- Daily backup to a hard drive located within the building - Redundant hard drives installed in servers for Patterson Imaging - Redundant hard drive cannot be done in IMAC - No current off-site backup	- Develop secure off-site backup - Privacy Impact Assessment required
4.19	Function knows and can implement Practice disaster recovery plan when required.	- Staff have access to computer tech's contact information	OK
4.20	Function minimizes duplicate recording of health information in its systems and records whenever possible.		OK

F. Develop Information Privacy and Security Policies

This process is outlined in the **Guide for Developing Information Privacy and Security Practice Specific Policies, which** is **Step 3.** It includes template documents that can be used to assemble a complete set of policies consistent with the *Health Information Act*. This sample set of policies is based on recommendations included in the Alberta Dental Association and College Standards, the Office of the Information and Privacy Commissioner of Alberta: Privacy Impact Assessment Requirements and the *Health Information Act*. Each section in the **Guide for Developing Information Privacy and Security Practice Specific Policies** is preceded by an explanation of the reason for the policy and a description of what should be included in the policies the practice develops.

The completion of the data collection templates: the **Site Privacy and Security Inspection template**, the **Health Information Registry template** and the **Practice Privacy Assessment template** will provide the information necessary to customize the **Information Privacy and Security Policies template** to a practice specific document during **Step 4**.

Quick point:

The development of Information Privacy and Security Policies is **Step 3** and is covered under the **Guide for Developing Information Privacy and Security Practice Specific Policies**

G. Privacy Impact Assessment

A Privacy Impact Assessment is an assessment of the custodian's compliance with the *Health Information Act*. The *Health Information Act* anticipates in most cases that a Privacy Impact Assessment will be filed by a custodian with the *Office of the Information and Privacy Commissioner of Alberta*. With respect to proposed new collection, use and disclosure of health information a resubmission of the PIA will be required unless the custodian decides that the change is only minor in relation to the policy or protocol previously adopted. It is always prudent if unsure to file an amended Privacy Impact Assessment. A custodian must prepare a Privacy Impact Assessment and must submit it to the Alberta *Office of the Information and Privacy Commissioner* prior to implementing the change in practice or system. This represents **Step 4** and is covered in the **Guide for Preparing Privacy Impact Assessment Submissions and Obtaining Information Manager Agreements.** For more information on Privacy Impact Assessments, see the Alberta *Office of the Information and Privacy Commissioner* website www.oipc.ab.ca

Quick point:

The development of Privacy Impact Assessment submissions to the *Office of the Information and Privacy Commissioner of Alberta* is Step 4 and covered under the Guide for Preparing Privacy Impact Assessment Submissions and Obtaining Information Manager Agreements