ALBERTA OCCUPATIONAL
HEALTH NURSES ASSOCIATION

PRIVACY AND CONFIDENTIALITY GUIDELINES FOR OCCUPATIONAL HEALTH NURSES

THIS PUBLICATION IS FOR INFORMATION PURPOSES ONLY AND SHOULD NOT BE CONSTRUED AS LEGAL ADVICE FROM ANY LAWYER, CONTRIBUTOR OR THE AOHNA. READERS SHOULD CONSULT LEGAL COUNSEL FOR SPECIFIC ADVICE.

Published by
Alberta Occupational Health Nurses Association (AOHNA)
Alberta, Canada

First edition 2006
Printed in Canada

TABLE OF CONTENTS

DEFINITIONS

Affiliate:	An employee, volunteer, agent, outsourced service provider, or information manager (subject to additional conditions) completing activities or functions on behalf of a custodian.
Authorized Representative:	A person who has been assigned to represent another individual, and to exercise the rights of the individual on their behalf. Persons recognized as having this status varies with the legislation, but generally includes: • Guardian of a minor. • Personal representative for the administration of a deceased individual's estate. • Guardian or trustee under the *Dependent Adults Act.* • Agent under the *Personal Directives Act.* • Attorney under power of attorney. • Nearest relative of a formal patient under the *Mental Health Act*. • Person with written authorization from the individual to act on the individual's behalf.
Breach:	An unauthorized disclosure, loss, or modification of information.
Collection:	Gathering, acquiring, receiving, or obtaining information.
Confidentiality:	Confidentiality is a condition under which information is not disclosed by a person or organization to others. Preserving confidentiality is one means by which an organization protects the privacy of individuals.
Custodian:	An organization or health professional designated under the *Health Information Act* (HIA) that is subject to the obligations and powers set out in the HIA. Custodians under the HIA are identified as Alberta Health Services, Alberta Health and Wellness, nursing homes, ambulance operators, as well as health professionals who are registered members of: • Alberta College of Pharmacists • Alberta College of Optometrists • Alberta Opticians Association • Alberta College and Association of Chiropractors • College of Physicians and Surgeons of Alberta • Alberta Association of Midwives • Alberta Podiatry Association

- College of Alberta Denturists
- Alberta Dental Association and College (after March 1, 2011)
- College of Registered Dental Hygienists of Alberta (after March 1, 2011)
- College Registered Nurses of Alberta (after September 1, 2011)

Custodians are responsible to comply with the HIA for any health information under their custody and control. This includes all health information they or their affiliates collect, receive, or disclose as part of the custodian's mandated functions and operations.

Disclosure: Release of information to individuals or agencies, usually outside of the organization, that are not normally authorized to access the information, in line with policy and legislative standards.

Health Information: Health information is a type of personal information generated as part of providing a health service to an individual. Under the HIA, it is personal information about any aspect of the physical or mental health of an individual collected while providing health services including health prevention, diagnosis, treatment, rehabilitation, and long-term care. Health information comprises diagnostic, treatment and care information, health provider information and registration information. However, health information generated for employee occupational health purposes as outlined in the HIA Regulations. 3.1 is excluded from this definition in the HIA.

Employment Management: As defined in PIPA, establishing, managing, or terminating an employment or volunteer relationship between the organization and the individual. Personal information created or kept as part for these purposes follow special collection, use and disclosure rules for Personal Employee Information.

Personal Information: Personal information is any factual or subjective information, recorded or not, about an identifiable individual, such as name, birth date, gender, address, education, employment, income, medical history, opinions, evaluations, or comments. It may also include information such as physical description, habits, personality, leisure activities or professional memberships or licenses. It includes recorded opinions of an individual as well as opinions about the individual.

Privacy: Privacy is the right to be left alone. In practical terms, it is the ability of individuals to control access to their personal information in the custody or under the control of others through accountability, consent, security, right of access, and regulation.

Reasonableness: What might be considered appropriate by a reasonable person in each situation. Its role in access and privacy legislation is to shed light on whether the practices of organizations are compliant with the provisions related to the collection, use and disclosure of

personal information. It may be assumed that an organization has collected, used, or disclosed personal information in a reasonable manner when:

- the organization can demonstrate that the collection, use or disclosure is necessary to meet a specific occupational health need. For example, the information was shared with a health specialist to facilitate the assessment of the client.
- the organization can demonstrate that the action was likely to be effective in meeting that need. For example, the personal information was collected to register the individual into a program of care.
- the collection, use or disclosure is proportional to the magnitude and importance of the problem. For example, when registering a patient to a health care facility, it is reasonable that only the information required to meet the activity is required (name, date of birth, family physician, health history, personal health number). The collection of credit card information or whether the individual is receiving social benefits would not be required to facilitate the task and would not be considered reasonable for the purposes of registering a patient.

The organization can demonstrate that there was no less privacy intrusive way of achieving the same end. For example, the occupational health nurse will only disclose a general assessment of fitness to work to a supervisor but will disclose much more specific health information to a specialist completing an independent medical examination.

Security: The processes, tools and measures used to identify threats and risks to the confidentiality or integrity of information, and implement administrative, physical, and technological means to combat those threats and risks.

Use: Release or sharing of information within the organization that is authorized by policy or law.

WHO SETS THE PRIVACY RULES FOR OCCUPATIONAL HEALTH NURSES?

Privacy Legislation and CRNA Code of Ethics

Quick Point: *Professional ethics standards under the College of Registered Nurses of Alberta (CRNA) are now completely in line with legislative requirements governing occupational health nurses.*

The nursing profession has a long history in safeguarding the confidentiality of personal health information as a vital component of their professional relationship with patients. A Code of Ethics for Registered Nurses in Canada has been adopted by the College of Registered Nurses of Alberta (CRNA) which governs registered Occupational Health Nurses (OHNs) in Alberta. The section on Privacy and Confidentiality provides high-level direction on major aspects of privacy (*Insert 1*).

Generally, privacy standards in legislation are paramount over professional ethics and codes of practice, but only if they are in conflict. The CRNA Code of Ethics is completely in line with current privacy legislation standards for health information across Canada, and in particular, the *Health Information Act* (HIA) of Alberta.

Insert 1: Code of Ethics for Registered Nurses

Maintaining Privacy and Confidentiality

Nurses recognize the importance of privacy and confidentiality and safeguard personal, family and community information obtained in the context of a professional relationship.

Ethical responsibilities:

1. Nurses respect the right of people to have control over the collection, use, access, and disclosure of their personal information.
2. When nurses are conversing with persons receiving care, they take reasonable measures to prevent confidential information in the conversation from being overheard.
3. Nurses collect, use, and disclose health information on a need-to know basis with the highest degree of anonymity possible in the circumstances and in accordance with privacy laws.
4. When nurses are required to disclose information for a particular purpose, they disclose only the amount of information necessary for that purpose and inform only those necessary. They attempt to do so in ways that minimize any potential harm to the individual, family, or community.
5. When nurses engage in any form of communication, including verbal or electronic, involving a discussion of clinical cases, they ensure that their discussion of persons receiving care is respectful and does not identify those persons unless appropriate.
6. Nurses advocate for persons in their care to receive access to their own health-care

records through a timely and affordable process when such access is requested.

7. Nurses respect policies that protect and preserve people's privacy, including security safeguards in information technology.
8. Nurses do not abuse their access to information by accessing health-care records, including their own, a family member's or any other persons, for purposes inconsistent with their professional obligations.
9. Nurses do not use photo or other technology to intrude into the privacy of a person receiving care.
10. Nurses intervene if others inappropriately access or disclose personal or health information of persons receiving care.

Are OHNs Now Covered Under the Health Information Act?

Quick Point: *Nurses are subject to HIA either as custodians or because they work for another custodian such as AHS as an affiliate under HIA. However, OHN assessments for fitness to work and benefits coverage are NOT covered by HIA because of the occupational health "carve out" in the Act.*

Step 1: Am I a custodian or an affiliate of a custodian?

To determine whether you and the health information you are handling is subject to HIA, you first need to know whether you are a designated "custodian" under the Act, or if you are working as an affiliate of another custodian under the Act.

Before September 1, 2011, when new amendments came into effect, HIA did not cover OHNs working independently or as employees of non-health organizations. Now, OHNs working in such situations are considered custodians who must follow the provisions of HIA. If an OHN is providing services as an employee or contractor to another *custodian*, such as Alberta Health Services or a long-term-care provider, HIA applies to the OHN as well because they are an *affiliate* of the custodian. So, regardless of their status, OHNs are now always in some way subject to HIA when they collect, use, disclose, and protect health information as part of their work.

Step 2: Is occupational health information I produce and receive covered by HIA?

Even though OHNs are custodians, if not affiliates of custodians under HIA, much of the health information they generate and receive providing occupational health services is not covered by HIA. Any services provided by an OHN relating to assessment of employee fitness-to-work or benefits claims will NOT be considered a "health service" under HIA. Therefore, health information produced by these services will not be covered under the Act. This is known as the occupational health "carve out."

Are there any services completed by an OHN that may be covered by HIA, despite the occupational health carve out? Yes: generally, these include services that go beyond assessment for fitness-to-work and involve preventive health, treatment, or rehabilitation for employees.

Insert 2 provides a quick summary of the kinds of activities performed by OHNs within the continuum of care. Examples of health services not covered by HIA are in red; services still covered by HIA are in blue.

What does this all mean for OHNs? For the most part, it means that the *status quo* for privacy regulation still prevails: OHNs, in completing fitness-to-work and benefits claim assessments, will fall under the access and privacy legislation of their employer or the client organization for whom they are providing contracted services. For instance, OHNs at a private company, even though they are custodians under HIA, must follow the privacy rules under the *Personal Information Protection Act* (PIPA) for most of the health information they handle.

Insert 2: Occupational Health "Carve Out" from HIA: What's In, What's Out

Continuum of Care Functions

Health promotion, illness prevention	**Assessment for fitness-to-work**	**Assessment care as part of treatment and rehabilitation**
Wellness programs designed to facilitate and promote health of employees Management of Employee vaccination programs Employee infectious disease surveillance	Review, interpretation, or assessment by a health service provider, for health protection or fitness-to-work purposes, of: • Results of drug/alcohol testing using bodily substances. • Results from medical, health, biological monitoring/surveillance of an individual; or • Results from a medical or health assessment.	Treatment or rehabilitation of employees, if not covered by Workers Compensation Act, such as for duty to accommodate programs Participation in employer-sponsored emergency response services to respond to field accidents, for example
Reviews and assessments by Director of Medical Services under the Occupational Health and Safety Act	Independent Medical Examinations or third-party reviews used for assessing benefits or insurance coverage	

NOT covered by HIA ***Still covered by HIA***

Other Privacy Legislation

Quick Point: OHNs must follow the privacy legislation of their employers or clients when handling fitness to work and benefits coverage assessment information of employees.

For the most part then, OHNs will be following privacy standards set by other legislation than HIA (*see Summary, Insert 3*). To determine which legislation applies, you need to establish who has control of the personal information you are handling. If, for example, you are an OHN working for a private health services company and the individual client is paying for their services on their own or through a private benefits plan, your health services company has control over that information and is therefore governed by the rules of the *Personal Information Protection Act* (PIPA) Alberta. If, however, another of your clients is an employee of a school board for whom your company is the outsourced occupational health service provider, that school board has control over the information and the information is therefore governed by the rules of the *Freedom of Information and Protection of Privacy Act* (FOIP) Alberta.

Insert 3: Summary of Privacy Law Affecting OHNs

Legislation	Jurisdiction and Application to OHNs
Health Information Act (HIA), Alberta	Treatment and rehabilitation health Information of all employees, regardless of the application ofother privacy legislation to the employer. OHNs are "custodians" of the information. Excludes occupational health assessment of employee fitness-to-work or benefits coverage. This health information will be covered by privacy legislation applying to employer (see below).
Personal Information Protection Act (PIPA), Alberta	Occupational health fitness to work or benefits claims health information of most Alberta private sector organizations: *e.g., EnCana, ATCO, Canadian Tire* Does not include private sector organizations governed by HIA or FOIP, e.g., *pharmacies, physician clinics, nursing homes, seniors' lodges.*
Freedom of Information and Protection of Privacy Act (FOIP), Alberta	Occupational health fitness-to-work or benefits claims health information of Public Bodies including Government of Alberta, municipalities, schools, universities, health Regions, nursing homes, seniors' lodges: *e.g., Alberta Health Services, Alberta Environment, City of Lethbridge, Athabasca University, Red Deer Public Schools*
Access to Information Act, Canada Privacy Act, Canada	All information of Federal departments, commissions, or crown corporations (*e.g., HealthCanada, Canada Post Corporation)*
Personal Information Protection and Electronic Documents Act (PIPEDA), Canada	All personal information of federal works in Alberta: e.g., TransCanada Pipelines, TELUS, Calgary Airport Authority Transactions that cross the Alberta border: e.g., occupational health service information transferred to operations in Saskatchewan

KEY CONCEPTS AND PRINCIPLES

Privacy vs Confidentiality

Quick Point: *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.*

When they think about managing personal health information, health professionals often talk about protecting the *confidentiality* of their patients or patients' information. Used this way, confidentiality involves safeguarding information from unauthorized access once it comes into the custody of the health professional.

Information *privacy* on the other hand, has a much broader meaning. Privacy has been defined, generally, as the "*right to be left alone*" or to keep certain aspects of your life removed from public view. Living and working in a modern society, however, requires everyone to share information about themselves with people and organizations providing services to them, such as OHNs. In practical terms, then, information privacy is based on principles and measures aimed at giving individuals control over how others - and particularly health professionals - create, share, protect, and manage their personal health information.

To comply with current privacy standards, OHNs therefore need to go beyond just protecting the confidentiality of personal information they hold: they need to develop and participate in an ongoing privacy program that addresses accountability, information flow, right of access, and security.

Roles and Policies

Quick Point: *Each organization must designate a Privacy Officer responsible for implementing their privacy program, backed up by privacy policies and procedures.*

Privacy accountability means that an organization's privacy program responsibilities and policies are clear and transparent to the public and there is a person who has been assigned the role of Privacy Officer to be accountable for the privacy program. This person is named on all privacy notifications and will process Right of Access requests. In addition, the organization or custodian must develop and follow specific policies and procedures for implementing the privacy program.

OHNs, as employees or agents of an organization must assist in identifying and protecting personal information according to the organization's privacy standards. Due to the sensitive nature of occupational health information, they may be required to process Right of Access requests, as well as if the Privacy Officer is a member of the organization's Human Resources function.

Why is Privacy so Important to OHNs?

Quick Point: *It is more than just compliance with a legal obligation to avoid sanctions - good privacy practices prevent harm to employees and clients and directly support an essential component of successful practice: public trust.*

Quality of Care

A breach of patient confidentiality can result in significant harm to an individual, including long-term financial implications, compromised personal or professional reputation, and identity theft. If patients cannot trust OHNs with their most sensitive and personal health issues, they will refrain from being open and frank with them – and that means health providers won't have the crucial information they need to provide an appropriate level of care.

Legislative and Professional Compliance

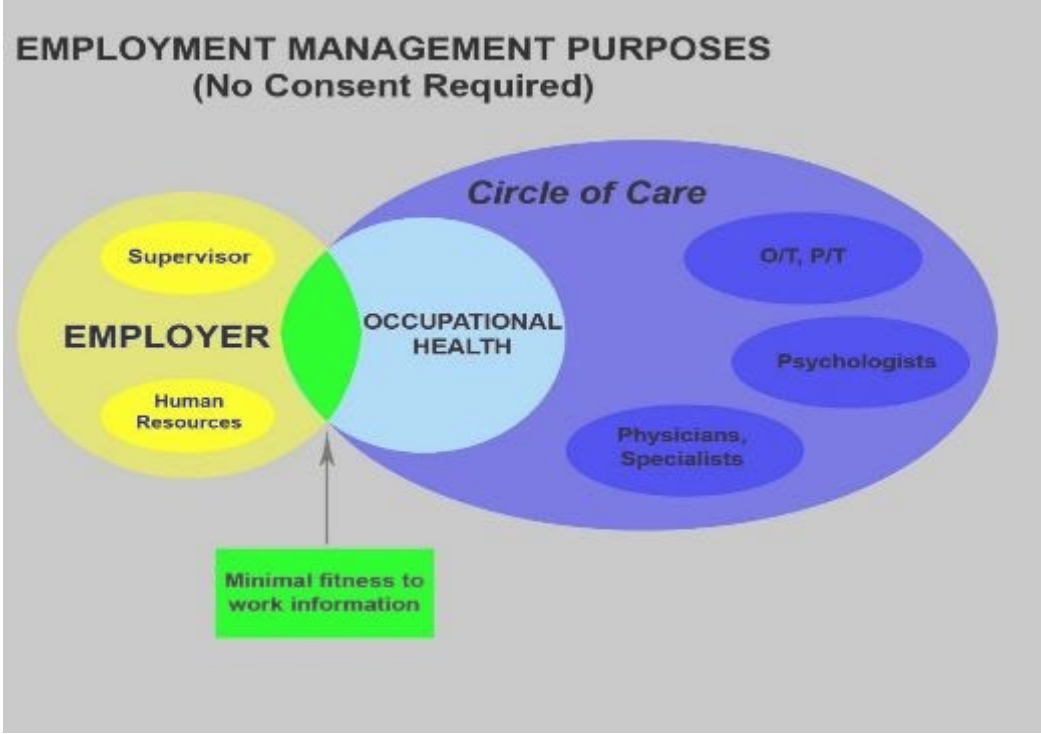
Compliance with laws is mandatory, and like all legislation, privacy laws stipulate sanctions for individuals or organizations who do not comply with their provisions. If a pharmacy professional fails to comply with the legislation, an investigation by the Information and Privacy Commissioner of Alberta may result in a review, investigation, or inquiry. Poor privacy practices can result in professional misconduct proceedings or other consequences. Sanctions for professional misconduct include reprimands, fines, imposing conditions on licenses, and suspending or revoking registration.

SHARING INFORMATION FOR EMPLOYMENT MANAGEMENT PURPOSES

Quick Point: *Except for the few OHNs in Alberta operating under PIPEDA, consent of the individual is not needed to collect, use, or disclose personal information of employees for Employment Management Purposes (EMP), including establishing managing or terminating an employment or volunteer work relationship.*

Occupational Health is considered an Employment Management Purpose and the personal information of the employee can be shared by the OHN for Occupational Health purposes without consent. The following diagram (*Figure 1*) outlines key occupational health stakeholders operating with within the employment management purposes (EMP) environment.

Figure 1: Collection, Use, and Disclosure of Occupational Health Information within an Employment Setting



In an employment setting, OHNs collect, use, and disclose person health information for employment management purposes. At the same time, their essential role as health providers means that sharing information with other health providers within the "circle of care" in any given case should be free- flowing to ensure complete and accurate health information is available. On the other hand, the exchange of health information between the OHN and the employer, including supervisors and Human Resources, for employment management purposes should be as minimal as possible and limited to minimal assessments regarding fitness to work and do not reveal medical conditions or treatments.

Insert 4 provides a typical scenario of how health information can be shared by and with an OHN for employment management purposes.

Insert 4: Sharing Health Information for Employment Management Purposes

An employer, as part of its disability management program, requires an Independent Medical Examination (IME) of an employee to determine whether their medical condition meets the criteria for long term disability coverage.

To support this objective, the employer's OHN (not the Supervisor or Human Resources) can request, receive, and review the full IME from a physician, and provide the physician with health information from the employee occupational health file to help complete the IME. Once they have reviewed the IME, the OHN can only provide HR or the Supervisor with a minimal report that the employee's condition meets or does not meet the insurance criteria.

Since the exchange of health information among officials in this example is limited to a legitimate employment management purpose, the employee must be notified, but their consent is not required.

COLLECTING, USING AND DISCLOSING OCCUPATIONAL HEALTH INFORMATION

Collecting Health Information

Quick Point: *OHNs should only collect and use the least amount of personal information required for the specific occupational health purpose, whether individual consent is required, and the individual is always notified of these purposes.*

The OHN's purpose for collecting personal health information whether that be for employment management or other reasons, should be established as clearly and completely as possible. Purposes for which personal information about employees can be collected for occupational health services include the types of activities described in *Insert 5*.

As a rule, OHNs need to limit the amount and type of information they collect to the least amount of health information needed to meet the needs of their occupational health function. For instance, OHNs do not need to collect SIN numbers of employees to provide services, nor should they be recording or charting opinions or information about other employees or family in their health records if it is not relevant to their assessment, monitoring or testing activities.

Insert 5: Examples of Occupational Health Purposes in an Employment Setting

- Monitoring the health of the employee through periodic, risk-based testing and to provide appropriate access to treatment as required.
- Assessing the employee's ability to perform a specific job, ability to return to work following medical absence, or specific medical restrictions.
- Processing or appealing claims for benefits or workers' compensation.
- Promoting and facilitating employee health and wellness.
- Supporting safety and loss prevention programs. Complying with occupational health and safety regulations.

Remember that most of these activities will be covered under the same privacy legislation governing the employer or client company, but some may still be covered by HIA (see *Are OHNs Now Covered under the Health Information Act?*).

Notification

It is important that OHNs notify the employee about the occupational health purposes up front in a clear, understandable form and to provide the name of an officer in the company or organization that can answer questions about the collection. This can be done through brochures, posters, or one- on-one consultations.

Indirect Collection

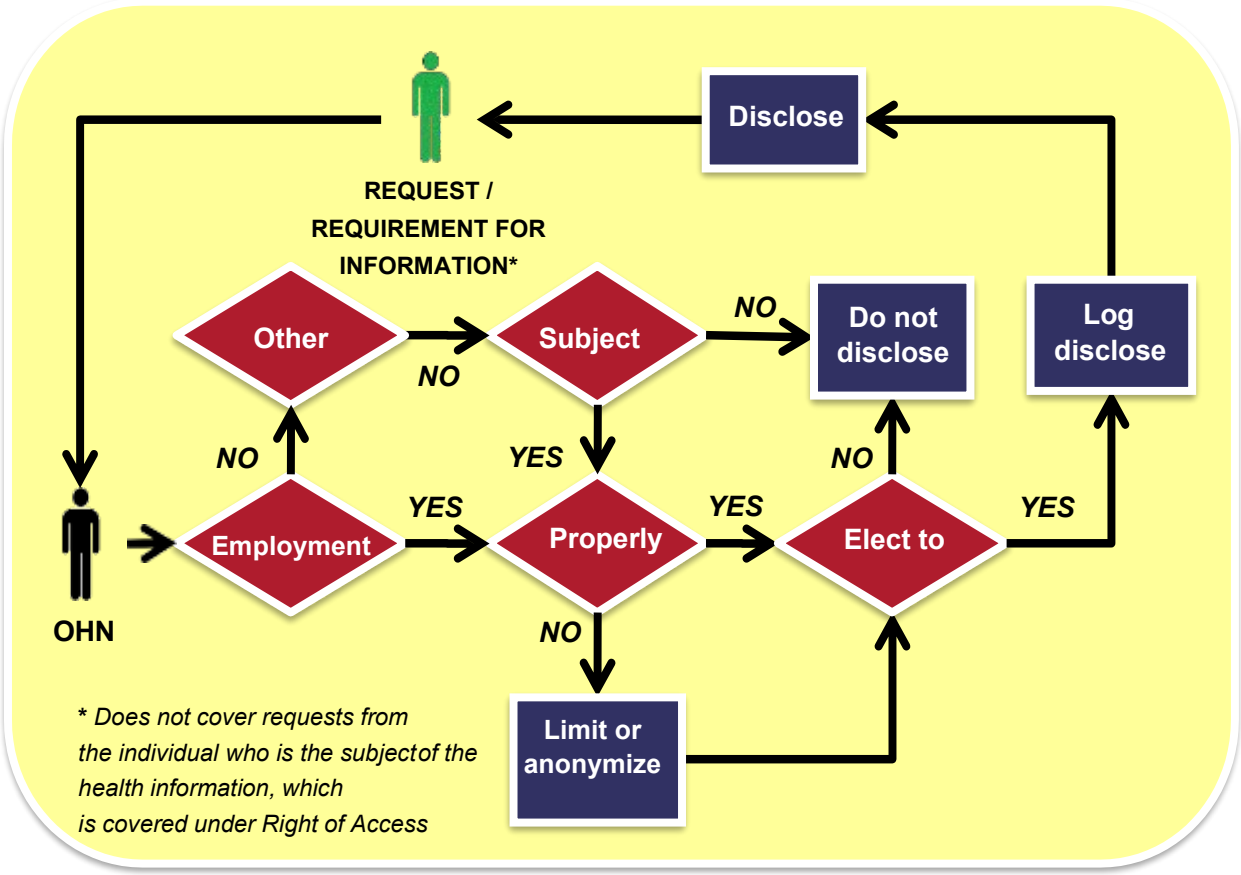
Generally, you should try to collect personal information directly from the client. However, especially to determine health status, it is often necessary to collect information from a family physician or specialist. This can be done without consent so long as the indirect collection is reasonably connected to the occupational health purposes under which you are providing services to the client.

Using and Disclosing Health Information

Quick Point: *For employment management purposes, OHNs disclose to a supervisor or Human Resources only minimal information, limited, for example, to whether the employee is fit to work and the conditions, if any, that need to be put in place to accommodate residual disabilities - no diagnostic or treatment information.*

The decision flow diagram below (*Figure 2*) provides a summary of the considerations an OHN might need to make under PIPA when their organization is requested or required to disclose occupational health information to a recipient outside of the organization. Note that this does not cover right of access requests from individuals who are the subjects of the information.

Figure 2: Disclosure Process Flow



Personal Information Protection Act (Alberta)

Personal information should be used by and disclosed only to those individuals for the occupational health purposes for which it was originally collected. Because occupational health information can so greatly affect the nature of the employment relationship, often to the detriment of the employee, occupational health professionals must be very careful to restrict access by the organization's human resources officials or supervisors.

For example, OHNs should not be releasing independent medical assessments or tests results in full to other company officials; rather, reports to the employer should be limited to a simple determination that they are fit-to-work and any specific work conditions that may be required to accommodate the employee.

Similarly, whenever personal health information is to be disclosed for occupational health purposes, such as to a physician or health provider providing an independent medical assessment, it should be limited to only information required for the assessment. In practical terms, OHNs need to judge this on a case-by-case basis since, for instance, working relationships and performance or even family status may have a significant bearing on the assessment for fitness-to-work.

Use and Disclosure for Purposes Other than Employment Management

When there is a request from internal investigators, legal counsel, family members or police, for example, to access health information beyond the normal occupational health activities, you may do so only with the consent of the client or under specific circumstances or exceptions identified in the relevant legislation. *Insert 6*, lists allowances for using and disclosing personal information without consent for purposes other than employment management.

Insert 6: Use and Disclosure of Personal Information for Purposes Other Than Employment Management and Without Consent

Personal Information Protection Act

- it is clearly in the interests of the individual and consent cannot be obtained in a timely way.
- it is for purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province when obtaining consent would compromise the availability or the accuracy of the information.
- as explicitly required or authorized by another law, bylaw, treaty, or legislative instrument.
- it is necessary to comply with a collective agreement binding on the organization under section 128 of the Labour Relations Code.
- to support statistical, archival, or scholarly study or research that cannot be achieved without using the information and consent is impractical.
- to support legal counsel to represent the organization.
- for the purposes of conducting an audit of the organization.
- to comply with a subpoena, warrant or court order.

- to a public body or a law enforcement agency to assist in a law enforcement investigation.
- to respond to an emergency that threatens the life, health or security of an individual or the public.
- to contact the next of kin or a friend of an injured, ill or deceased individual.
- to collect a debt owed or to repay money owed by the organization.
- the information is publicly available.
- to the surviving spouse or adult interdependent partner or relative of a deceased individual if reasonable.
- to determine suitability to receive an honour, award, or similar benefit.
- if it is reasonable for an investigation or a legal proceeding.
- to or by an authorized organization to protect against, or prevent, detect or suppress fraud.

Logging Disclosures

It is good practice to record all incidents of disclosure of individually identifiable health information. Disclosure logging shows what information has been edited or disclosed about a patient and to whom the information is disclosed.

These may be separate disclosure logs (paper-based or electronic) or may simply be any documentation in a record providing evidence of the nature of the disclosure and who the recipient was. Disclosure logs are critical when information is lost, manipulated in an unauthorized manner, when a recipient needs to be notified of a correction, or in the event of a breach of privacy. The application of disclosure logs supports accountability in the management of individually identifiable health information.

Forms of Consent

Quick Point: *Consent of the individual, when it is required, should be informed, clear, and, in most circumstances, explicit.*

Where consent is required, it must be part of a process where the employee is fully informed and not subject to unreasonable pressure to decide one way or the other. Consent, even if it is offered by the individual, should be requested only for reasonable purposes required by the OHN to deliver services.

Consents can take several forms:

Explicit consent: An individual is properly informed and explicitly gives you permission, either in writing or orally, before action taken. Written consent is preferred if the consent is questioned later but is not always feasible to obtain. For oral consent obtained over the telephone, recording the consent in the record, and having a witness participate in the conversation will enhance the effectiveness of the process.

Implied consent: Permission is reasonably implied based on the circumstances of the transaction. For instance, the employee intentionally and directly releases the information to you and the nature and purposes of the collection are so clear to the individual that they do not need to be stated or explained.

Opt-out: Sometimes call “negative consent.” An individual is given reasonable opportunity to express their wishes regarding a proposed collection, use or disclosure, usually by mail, e-mail, advertisement, or internet notification; if no response is given, consent is assumed.

Generally, given the sensitivity of health information within the work environment, where consent is required, it should be an explicit consent. Opt-out should be reserved only for collection, use, and disclosure of simple contact information of individuals.

A fully informed explicit consent should contain the following elements:

- An authorization from the individual or authorized representative.
- The purpose for collection, use or disclosure.
- The users or recipients of the personal information.
- An acknowledgement that the individual providing the consent understands the risks of consenting or not consenting.
- The effective date and, if any, the expiry date of the consent.
- A statement that the consent may be revoked by the individual at any time.

Consents are by nature voluntary, so the employee can refuse to consent, or withdraw a consent that they already given. If this occurs, the OHN is not required to destroy the information since it might be needed for evidentiary purposes, but must cease to collect, use, and disclose it for business purposes. The OHN should always, within reason, seek alternatives where they can still provide health services without the personal information. Of course, a minimum quality of care should never be compromised.

Be sure to get consent before you collect, use, or disclose information – a consent collected after the fact is not valid. *Figure 3* is a model form for written explicit consent.

Figure 3: Model Form for Written Explicit Consent

CONSENT TO THE DISCLOSURE OF INDIVIDUALLY IDENTIFYING HEALTH INFORMATION

AUTHORIZED BY THE HEALTH INFORMATION ACT (*HIA*), SECTION 34

CLIENT INFORMATION:

Name: _____
(surname) (given name/names)

Date of Birth: _____
(day/month/year)

Address: _____

I authorize my individually identifying health information related to _____

_____
(description of information/relevant dates, etc)

to be disclosed by _____
(name of custodian)

in accordance with section 34 of the *Health Information Act* to,

_____
(name of recipient)

for the following purpose(s): _____

_____

_____

I understand why I have been asked to disclose my individually identifying information, and am aware of the risks or benefits of consenting, or refusing to consent, to the disclosure of my individually identifying information. I understand that I may revoke this consent in writing at any time.

Dated this _____ of _____, _____. Expiry date (if any): _____ of _____, _____
(day) (month) (year) (day) (month) (year)

_____
Signature of client/authorized representative*

* if you are signing on behalf of the client, the following information must be provided:

_____ _____
Print Name of Authorized Representative **Print** Source of Representative's Authority [refer to *HIA* section 104(1)]

_____ _____
Witness Signature Witness Name

Revised June 6, 2006

INDIVIDUAL RIGHT OF ACCESS TO OCCUPATIONAL HEALTH INFORMATION

The Right of Access

Quick Point: *All individuals have a right of access to their own personal information – it can't be limited or waived except by legislation.*

A fundamental principle of privacy legislation is that individuals have right of access to their own personal information kept by any organization, including their employer. Patients may request information contained in their health record for any reason, including for the purposes of a dispute with the employer or benefits provider. It is more important, therefore, that the access process be designed from the outset to be open, consistent, and compliant with privacy standards in legislation.

Individual Requests for Access to Personal Information

Quick Point: *Don't use the formal right of access process if the information requested clearly doesn't require review to release. If it does, you must follow the formal 30 or 45-day process prescribed by the relevant privacy legislation, under the direction of the Privacy Officer.*

Requests from individuals to access basic personal or health information about themselves (e.g., test results, assessments, examinations) can be handled as a relatively informal, routine release so long as there is clearly no information in the record that will need to be withheld and the information can be accessed easily.

In all other cases, the request should be treated more formally which means they should be made in writing and forwarded to the Privacy Officer or another person responsible for this task in your organization. In such cases, the OHN may still be involved in processing the request and therefore should be aware of the request process.

It is important to note that only the individual the information is about has the right of access to the information. This doesn't include other family members or others, unless these people are "authorized representatives" of the individual in accordance with criteria set out the privacy legislation. There are other specific situations where access may be granted to people other than the subject of the information. OHNs, therefore, need to understand these restrictions / exemptions, make reasonable efforts to verify that requesters are who they say they are and to establish that the necessary authorization is in place.

Access and privacy legislation requires that the employer respond to formal requests for access to health information within a certain period - 30 to 45 calendar days, depending on the legislation. Although there are provisions for extensions of time limits, these provisions are specific in nature and include criteria that must be met by the employer (i.e., the request is so voluminous that extended time is needed to facilitate request processing).

Individuals should normally not be charged for access to their own personal information. However, reasonable fees may be charged for reproduction, transcription, or transmission of information, so long as the individual is notified before these costs are incurred. A fee for reasonable costs incurred may be charged when responding to more complex requests. The individual must be given an estimate of the fee in advance, and it must represent costs incurred, rather than being 'priced' as a service.

Requested information must be provided in a form that is generally understandable; organizations have a general 'duty to assist' someone requesting their own information. Occupational health professionals should explain the meaning of the records' content, such as any codes or abbreviations.

Individuals are permitted to either view the original record or to request a copy. To preserve the integrity of the record and ensure that documents are not removed from the premises of the employer, an individual wishing to view an original record usually does so under supervision.

Withholding Information from Individuals

Quick Point: *Privacy legislation identifies a limited number of mandatory and discretionary exceptions to an individual's right of access. If these exceptions do not apply, the information must be released.*

In certain situations, occupational health care providers may not be able to provide access to the complete record of personal information it holds about an individual.

Occupational health care providers must refuse to provide access to information when it is about another person unless the other person consents to the access. This, along with two other exceptions, is a mandatory provision in the legislation. In addition, there are several specific circumstances where the organization is given the discretion to withhold information as an exception to the right of access. Descriptions of the mandatory and discretionary exceptions recognized by PIPA are listed in *Insert 7*.

Insert 7: Exceptions to an Individual's Right of Access to Their Own Personal Information

Personal Information Protection Act

Mandatory: must not release information to the requestor when,

- the personal information is about another person.
- disclosure would threaten the life or safety of someone; or
- the information reveals the identity of someone providing a confidential opinion about the individual.

Discretionary: may not release information to the requestor when,

- it would reveal confidential commercial information.

- the information was collected without the individual's knowledge or consent as part of an investigation of a breach of agreement or contravention of law.
- it is protected by solicitor-client privilege.
- the information was generated in the course of a formal mediation or dispute resolution process; or
- it would likely result in the required information no longer being provided to the OHN.

If a file or document contains information that is not to be released, the information is either directly "severed" or taken out so that the rest of the file or document can be released. You must inform the requestor that information has been withheld, severed, or manipulated, and state clearly the reason for this in relation to the legislative exception. You must also instruct the individual on the avenues available to challenge the decision. Encourage the applicant to first bring their complaint or concern to your organizations' Privacy Officer. If this is unsuccessful, the applicant can make a formal complaint to the Information and Privacy Commissioner of Alberta or the Privacy Commissioner of Canada, depending on the privacy law that applies (see Dealing with the Commissioner's Office below).

Requests to Correct or Amend Health Information

OHNs have a duty under the legislation to collect, use, and disclose personal information that is as accurate and complete as reasonably possible. Individuals have a right to request correction of personal information held by an organization.

As with requests for access, requests from individuals to correct or amend basic health registration information about themselves (e.g., change of name or address) are handled as a routine release of information.

Formal requests to correct or amend personal health information must be in writing to the office designated to administer access requests. An individual may request a correction to another person's information only if they have that person's signed consent, or proof that they are a legal representative of the individual. Formal requests for correction of personal health information must be processed within 30 days of the time the request is received.

All formal requests must be accompanied by appropriate documentation to support the request before the employer will amend the information as required and as appropriate. Generally, the employer will not amend professional opinions that are made by occupational health care staff who have the competency to make them. If amendments are made, the original information must not be deleted but retained and marked as incorrect by crossing out.

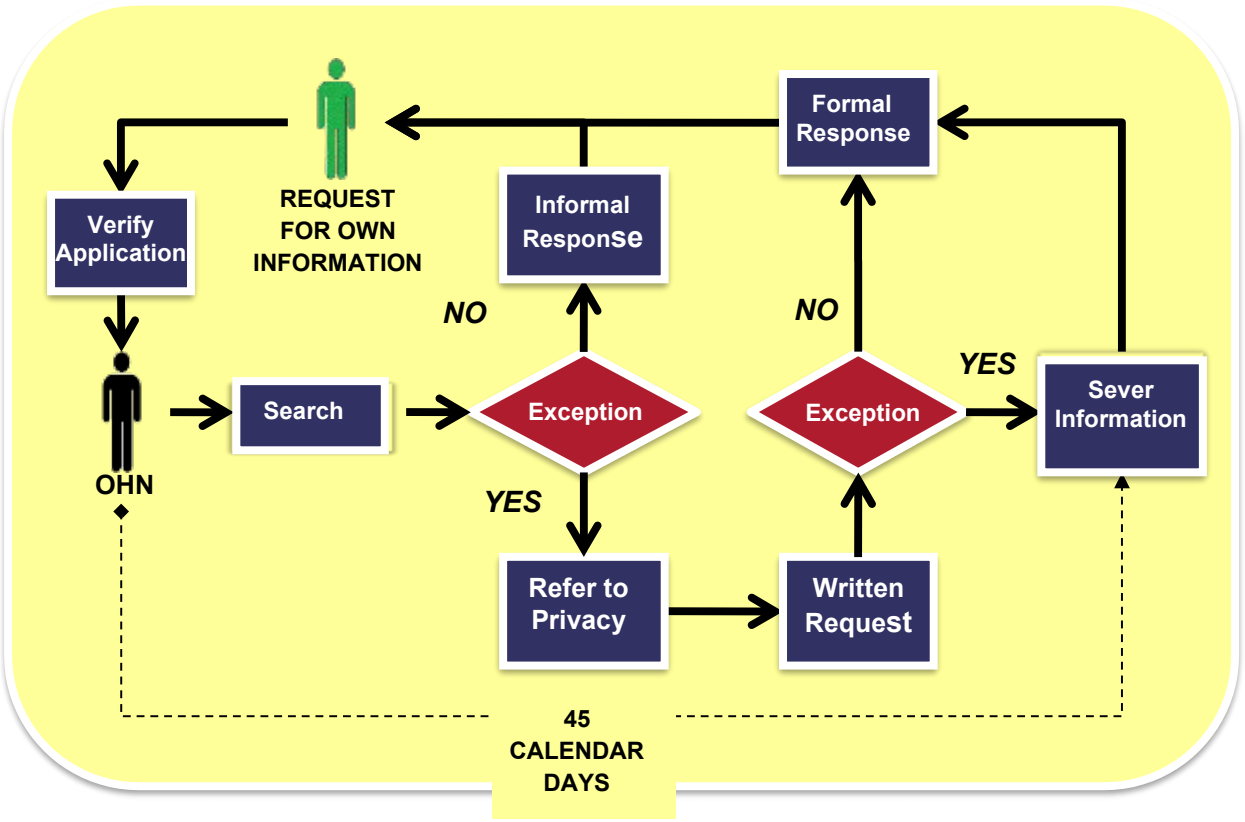
The amended information will be transmitted to third parties, as appropriate, usually to those who had received the incorrect information within one year of the correction or amendment is made.

Individual Access Summary

The diagram below (*Figure 4*) summarizes the decisions and steps needed to properly process a right of access request under PIPA.

Figure 4: Right of Access Process Flow

Personal Information Protection Act (Alberta)



SECURING HEALTH INFORMATION

The Need for Information Security

Quick Point: *Because health information is so sensitive, OHNs need to institute and maintain a comprehensive information security program for protecting the confidentiality and integrity of health information in their custody and control.*

Personal health information ranks very high in sensitivity and can result in serious repercussions to the individual whom the information is about if the information is breached. Occupational health professionals need to secure personal health information from unauthorized collection, use disclosure or destruction using all reasonable administrative, physical, or technical means at their disposal.

Some specific tips for implementing security for personal information in your area:

- Adopt a clean desk rule. Clear off work area at the end of each day (or when leaving your work area for an extended period) and lock records containing personal information in desks, cabinets, safes, or rooms.
- Log-off systems that contain personal information when you are away from your work area.
- Ensure that files containing personal information are protected using passwords. Any such passwords should not be disclosed, recorded in areas accessible by others and should be changed on a regular basis.
- Take all necessary steps to ensure that any electronic records contained on your hard drive are backed-up at regular intervals.
- Ensure that records containing personal information are not saved on an unprotected-shared drive.
- Mail personal information using securely sealed double envelopes stamping the inside envelope CONFIDENTIAL and identifying the intended recipient.
- Erase boards and remove documents, drawings, flipcharts, and other records containing personal information from meeting areas.
- Avoid leaving records containing personal information in reception areas, and other public places.
- Personal information should not be posted or made viewable by the public or by employees.
- Lock file rooms and computer rooms.
- Lock exterior doors after hours – or even during business hours, if appropriate – and do not prop open locked doors.
- Register and escort visitors/vendors and restrict casual visitors to designated areas.
- Ensure protective measures are taken when keeping records with personal information at home or in transit.

- Take all necessary precautions to prevent the theft of equipment (such as laptops, PDAs) to avoid disclosure of personal information to unauthorized persons.
- Avoid the discussion of personal information in public places such as lobbies, elevators, restaurants, train stations and airplanes. Discuss issues about an identifiable individual behind closed doors and refrain from using speakerphones, as others near by may not be privy to this personal information.
- Personal information is particularly vulnerable at the time of destruction. Ensure that both paper and electronic media containing personal information are fully destroyed beyond recovery before they leave your secure custody.
- Avoid copying or retaining records on the sole basis of convenience or "just in case" logic; make certain that copies are destroyed quickly and securely.
- Retain and destroy master copies of records only in accordance with pre-determined retention periods and documented scheduling processes. Do not destroy information that is the subject of a current request for access.

Service Provider Agreements

A company or organization that outsources or contracts with an outside agency for occupational health services must ensure that the service provider's practices are compliant with the legislation that applies to the contracting organization. You may be the contracted service provider or may be responsible for overseeing occupational health service providers at your company. In either case, the occupational service provider should have in place polices and processes that meet relevant privacy and security standards. Both parties should be obligated to meet these standards in their service agreements.

Breach Responses

When an information security breach or violation has been discovered, identify the level of the incident. Specific policies for employers may vary. However, some general steps that should be undertaken by occupational health professionals includes the need to:

- Confirm the breach or violation and the level of gravity.
- Take all necessary steps to prevent further breach of the information, including retrieval of breached records from any unauthorized recipients.
- Report the information security incident to the privacy officer. The person handling the breach should consult with staff as needed on a case-by-case basis to determine whether it is appropriate to inform the subject of the breach.

Some things to consider:

- if it is evident that the breach presents a danger to the subject.
- if the quantity of information and subjects involved in the breach is significant.
- if the recipient of the breach has or is likely to contact the subject; or

- if the recipient will not destroy or return the information.

Generally, if it is a significant breach, it is appropriate to inform the employee that their information has been breached. Do not inform the subject if it is determined that disclosure of the breach would likely harm the subject.

Occupational Health Record Retention

Occupational health records should be segregated from employee files and meet health records standards in terms of objective charting, accuracy, and completeness. Establish a clear policy and schedule for retaining occupational health records. There are several legislative and professional retention standards that will need to be considered:

College of Physicians and Surgeons of Alberta

The College of Physicians and Surgeons' policy on retention of health information records may be used as a guideline for OHNs. The policy recommends that patient records be retained for a period of 10 years from the last date of service. Diagnostic images on film should be retained for a minimum of 5 years. All other records should be retained for a minimum of 10 years. In the case of minors, patient information should be retained for at least 2 years after the individual becomes the age of majority (18 years of age) or 10 years, whichever is longer.

Alberta Occupational Health and Safety Act (Safety Code)

Section 220(1) of the *Occupational Health and Safety Code* requires that results of noise exposure assessments of employees be conducted on a regular basis. Information concerning the dates and individuals tested, types of equipment used, levels of sound measurements and location of the assessment must be recorded. The record of the assessments must be retained for as long as the employer continues to operate in the province.

Under section 40(1) employees subject to hazardous materials such as asbestos, coal dust or silica must undergo a full medical assessment. Once the assessment has been completed, a recording of the evaluation including employee name and identifying information, the tests performed (x-rays, etc.) and interpretation of the results by the attending physician must be documented. In conjunction with the Act, the information must be retained for a period of not less than 30 years.

Limitations Act

Employers should be aware of the potential for complaint or litigation in the event an occupational health incident or investigation. In these cases, the employer should retain records of the incident, particularly information concerning the health of the individual.

Section 3(1) of the *Alberta Limitations Act* provides that for claimants to successfully seek a remedial order for an injury, it must be carried out within 2 years after the date on which the claimant first knew of injury or should have known of the injury. As well, if 10 years pass after the claim arose then the defendant is entitled to immunity from liability in respect of the claim. As a result, employers should retain records of work-related injuries,

accidents, or investigations for a minimum of 10 years after the resolution of complaints and/or investigations are fully resolved. In the event of hazardous materials incidents, the records would need to be retained in accordance with required retention provisions.

Transferring Custody of Information Holdings

There are legislative provisions for the transfer of records arising naturally from changes in organizational status and structure. Under HIA, records may be transferred to a "successor custodian" without consent. Under PIPA, records necessary for evaluating or completing a "business transaction" resulting in a change in ownership, such as an acquisition or merger, may be disclosed/collected without consent. Parties must enter into an agreement to dispose of, or return, information should the transaction not proceed and to restrict use to this narrow purpose. (For example, whereas providing access to payroll details or operational safety records is reasonable, disclosing ordinarily confidential OH information is not.) Under FOIP, nothing prevents public bodies from transferring custody among them, without consent, provided mandates are sufficiently aligned so that they are each using the information for the originally legitimate purpose. As with any disclosure or disposition, you should document a transfer of custody.

Of course, if the transfer is one of the final acts of the entity before wind-up, the question of custody and responsibility becomes problematic. The organization being dissolved has responsibility for the protection and proper disposition of the records, but if this neglected, there is little recourse. The College of Physicians and Surgeons, for instance, does not have a custodianship program in place to house patient records of "abandoned" practices, although the practitioner is expected to ensure that records are disposed of properly.

Electronic Records

Computing technologies enable large volumes of personal information to be collected, stored, used, and disclosed in a short period of time, much to the support of occupational health services. It is important to remember, though, that electronic health information must be managed and protected as a strategic resource, much the same way as paper-based information is.

Electronic records can be added to or manipulated without any readily identifiable evidence of such changes. It can also be easily disclosed to third parties with a press of a keyboard button. As a result, it is advisable to make information technology staff aware of the information to assist in creating security measures such as password protected systems, encryption, and access audit logs to mitigate outside access to the information and ensure adequate monitoring. Electronic records should be disposed in accordance with the retention periods established for non-paper records.

Fax and e-mail Security

Fax and e-mail are not very secure methods for transmitting health information, yet their use is widespread. Here are some tips for make these transmissions as secure as possible:

For all transmissions:

- Limit use to circumstances where it is immediately necessary for time-sensitive or functional reasons and to the least amount of information possible.
- Include a banner or notice about the confidentiality of the information and a contact should the information be received in error.

For fax transmissions:

- Confirm fax number by phone prior to sending transmission.
- Ensure that the recipient's machine is in a secure area. Otherwise, the recipient should stand by to receive and confirm transmission of the information.
- Use an approved cover sheet.
- To ensure accuracy in dialing, confirm the number being dialed by visual check on the fax machine display. For frequently dialed numbers, use the automatic dialing feature to minimize incorrect dialing.
- For automatic faxing by computer, use a fax table for automatic dialing of numbers.
- Faxed information, which is transferred from a central fax area (switchboard to a patient/client area), should be sent in a sealed secure manner to the patient/client care area.
- Print out and check the fax machine logs after transmission to verify that documents were received at the correct number.
- If it is determined that the transmission was received by a wrong number:

  (a) contact the recipient and ask them to return or destroy the documents;
  (b) retain copies of all information sent; and
  (c) report the incident as an information security breach.
- Display these procedures at every fax machine in your area.

For e-mail transmissions:

- Do not transmit by e-mail over a service other than the corporate e-mail service (e.g., Hotmail).
- Remove or code all personal identifiers from the message.
- Do not transmit identifiable personal information by e-mail to an external or public network unless the information is secured by encryption.
- Do not include identifiers or personal information in the subject header of the mail.
- Verify all addresses as correct before sending messages.
- Develop, update, and use e-mail addresses from address book.
- Request notification of receipt.

DEVELOPING AND IMPLEMENTING A PRIVACY PROGRAM

Privacy management requires effective knowledge, control, and accountability of the personal information in your area of responsibility. This section discusses some of the tool and methods for defining, managing, and evaluating privacy compliance.

Gap Assessment

A first step in undertaking a privacy program for occupational health information involves conducting a gap assessment. A gap assessment can be used as a first step in determining which areas of the organization require improved business practices to better comply with provisions regulating the collection, use, and disclosure of personal health information. A business plan should be developed to manage the privacy of personal information in the organization.

Privacy and Security Policy

A privacy policy is an important aspect of an organization's ability to comply with privacy legislation. Privacy policies inform both staff and members of the public that privacy is recognized and respected by the organization.

The policy should include steps for informal and formal disclosures of personal information and to whom requests are to be forwarded. The policy provides direction on the kinds of records that may be available outside the legislation, the delegation of authority (who has responsibility for decisions under the legislation) and what records might constitute an unreasonable invasion of privacy if disclosed without consent.

Privacy policies provide an established direction for each employer on question concerning consent for collection, use and disclosure of personal information, how personal information is to be managed, and the steps to be followed in the event of a breach of personal information.

The Role of the Privacy Officer

When an organization receives a formal request for access to information, or there is a breach of personal information, the request or investigation is usually completed by the organization's designated privacy officer – a position required by legislation. As part of this process, the privacy officer will need to compile all information relevant to the request or the breach investigation, which may include occupational health information. OHNs may be hesitant to release extensive occupational health information to a non-health provider, but it is allowable and, arguably, required by the privacy law under rules for organizational accountability and duty to assist.

At the same time, organizations should consider the special role of occupational health in their organization when choosing a privacy officer. A privacy officer should have sufficient scope of authority and independence to ensure that other officials will not need to access information in

the custody of the privacy officer. In addition, the privacy officer should be as free as possible from conflict-of-interest situations.

Many private sectors organizations, for instance, have designated a high-level human resources official as privacy officer, which presents particular risks if those human resources official need to access occupational health information of an employee to deal with a request. In such circumstances, OHNs could suggest that an occupational health staff member be made responsible and trained for processing requests for access to occupational health information.

Training

Staff training is an important aspect of compliance with privacy legislation. Staff need to understand the importance of and value of personal health information, why it needs to be protected from unauthorized collection, use, disclosure, or destruction and what the repercussions are for such practices. It is recommended that the trainers design levels of training for designated groups within the organization. For example, secretarial and other support staff may not receive the same level of training, as would occupational health nurses who work with personal health information on a day-to-day basis.

Dealing with the Commissioner's Office

Depending on the jurisdiction, the Information and Privacy Commissioner of Alberta or the Privacy Commissioner of Canada may become involved regarding a response to their request for access or correction or any other issues relating to collection, use, disclosure, and security of personal information. In a typical case, the Privacy Officer will be the one directly involved in dealing with the Commissioner's Office officials, but an OHN may also have a role in this process.

In the case of a complaint from an individual, the Portfolio officer will work with both your organization and the complainant to try to come up with a reasonable mediated solution. If this is unsuccessful, the case may move to a formal inquiry process, in which both parties present their cases and the Commissioner delivers a finding or ruling which, in Alberta, is binding. It is therefore important to document your privacy policies and processes clearly to ensure that you are well represented in any review and inquiry process that may arise.

Privacy Tools

Privacy management requires effective knowledge, control, and accountability for the personal information in your area of responsibility. Several tools are available to help you assess privacy compliance in business processes.

Personal Information Registry (PIR)

A PIR involves identifying repositories of personal information, where they are and how they are to be managed. A key goal of the PIR is to identify accountabilities on information collection, use, disclosure as it applies to systems that support personal information creation, access, processing, disclosure, and storage.

An example excerpt from a Personal Information Registry can be found in Appendix 1.

Privacy Impact Assessment (PIA)

A PIA is an assessment of the compliance of new or changed business systems, practices, or processes with privacy regulations.

A PIA completed just as a system or change is implemented will tend to result in an assessment that is accurate, but that identifies issues too late to address them thoroughly and efficiently.

A more proactive and privacy-enhancing approach to PIAs is to integrate privacy regulations, standards, and concerns into the early stages of development. Not only can more robust and ambitious privacy objectives be established, but they will also almost certainly cost less to achieve if 'designed in.' Money and time are only two types of avoidable losses; late stage, 'inspection-style' PIAs can also produce irresolvable compliance issues that force a choice between tolerating a known risk (leaving 'as is') or foregoing intended system functionality (turning something off).

In either case, the assessment is based on applying the relevant privacy standards (which may arise from multiple sources) to some description or model of the system (whether as-proposed or as- built). Privacy standards may, indeed, be perceived as obstacles by other project stakeholders; likewise, to the privacy advocate, some business objectives can seem ominous. But the most valid and useful assessments result from a truly mutual understanding of relevant aims and constraints. Like any other collaborative effort, effective PIAs begin with early, open, and affirmative communication about organizational change.

An example excerpt from a Privacy Impact Assessment survey tool can be found in Appendix 2.

FREQUENTLY ASKED QUESTIONS

What privacy legislation must an OHN in Alberta follow when collecting, using, disclosing, and protecting the health information they create and receive?

It depends on the nature of the activities for which the health information is created and the status of the employer or client company on whose behalf those activities were performed.

The *Health Information Act* will NOT cover health information created by OHNs to assess employee fitness to work, to review health safety, or to support disability management. This is called the "occupational health carve out" in the *Health Information Act*.

Health information within the occupational health carve out would instead need to follow the legislation that applies to the employer (private company - *Personal Information Protection Act*; public body - *Freedom of Information and Protection of Privacy Act*).

Some health information created by OHNs would likely NOT be covered by occupational health carve out and therefore would still be under the *Health Information Act*. Generally, this would include health information generated as part of direct treatment activities, such as vaccination campaigns, rehabilitation work, or even workplace wellness programs.

If there are different privacy laws for different provinces and sectors within provinces, which rules does an employer's policy follow in managing its occupational health information?

While Canadian privacy law is consistent in its objectives and basic principles, there are some differences in the areas such as consent and coverage. A consistent best practices approach based on the highest standard of all applicable Canadian privacy legislation covering employee health information should be used. This means that the employer's policies and practices for handling occupational health information is consistent across Canada and compliant with legislation in any jurisdiction.

Am I obligated to show an employee all his or her health information?

Under law, an employee has a right of access to all health information about them. However, there are a few circumstances where this right of access is limited, such as when access would threaten the health or safety of someone or would reveal personal information of another person.

If an employee has access to all their information, is there a need to avoid recording potentially controversial information, or at least recording it somewhere other than the employee health record?

Right of access should never be used as a reason not to collect information necessary to provide high quality health services to an employee. However, there are some basic principles that may help to ensure that the information you are recording is accurate and understandable. All personal information contained in notes or reports should be:

- objective and based on observable facts or reasonable conclusions,
- accurate and complete,
- free of extraneous or unsubstantiated remarks, and
- restricted to one individual as much as possible.

Storing contentious, sensitive, or controversial personal information outside of the employee health record will not protect it from either the employee's right of access or the requirement to notify the employee of its existence.

What about severing? How is information severed from a record?

Severing is the process of removing information from a record. Severing must be exercised via legislated reasons, prior to removing information from the record. Each statute includes exceptions to disclosure of information provisions. These provisions authorize the decision-maker to withhold information from an applicant. The specific sections used to withhold the information must be indicated on the record to enable the applicant to understand the basis upon which the information was removed and withheld.

Am I obligated to get permission before I disclose reports received from doctors or specialists that are marked "do not release without the permission of Dr. XYZ"?

Doctors or specialists cannot limit the employee's right of access to their own health information contained in a report. However, such markings may indicate that the doctor has concerns about harm to the employee if this report is released to them - confirm this with the doctor before release.

Should I segregate the occupational health information of employees?

Yes. The occupational health information should be maintained separately from the employee personnel file. Access to the employee file does not provide a basis for access to the occupational health record. The occupational health information needs to be accessible but should be retained separately from other employee information in one designated place.

What about charting – do I need to take precautions?

Note-taking and updating charts encompass occupational health information of the employee and form part of the occupational health record. The information should be managed in accordance with the principle of the limitation on sharing of personal information. Any reporting involving the use of employee occupational health information should be exercised with the highest degree of anonymity possible.

Can family members or others working on behalf of an employee have access to the employee's health record if required?

Family members do not have access to an employee's file unless they have the express consent of the employee or have the status of guardian, trustee, or legal representative of the employee. Some health information may be released to a family member where someone's life, health or security is threatened. For example, if an employee declares a clear intention to seriously harm the family member and the threat is imminent.

Others working on behalf of an employee, such as a lawyer or union representative, can only be given an employee's health information with the employee's consent.

What if the employee is deceased?

Restrictions on access to an employee's health information do not lapse with the death of the employee. A surviving spouse may have access for insurance or benefits purposes only if they are executor or with the consent of the executor of the employee's estate or, under some legislation, if you think the disclosure is reasonable.

How do I handle information of former employees?

Even though the employee may have left the organization, the personal health information should only be shared on a need-to-know basis. The privacy provision continues to apply to the information if it is in the custody or under the control of the employer.

It is important, therefore, to establish a retention policy for occupational health information. The *Alberta Labour Relations Code* requires a retention period of at least 3 years after termination. However, it is advisable to maintain some employee health information for at least 10 years, especially employees with health problems affecting or relating to their work, to support any claims made against the company within the time limits established under the *Alberta Limitations Act*.

What health information can I disclose to an employee's manager or supervisor?

Occupational health professionals provide managers or supervisors with the least amount of health information required to fulfill employment and safety functions consistent with the employee's consent, including:

- Fitness to work report as mandated by statute
- Notice that a medical condition exists, and that the employee is under medical care
- Time that the employee has been, and is expected to be, off work
- Medical restrictions on the type or amount of work or specific tasks to ensure employee safety and effectiveness

All other releases of employee health information to managers or supervisors require specific consent of the employee.

What about health information collected as part of Employee Assistance Programs (EAP)? Is this part of the Occupational Health services operated by an OHN?

EAP is generally considered a benefit for the employee and not a service for an employment management purpose. Employees will decide with EAP counsellors directly; neither the OHN or the supervisor need to know which employees have accessed EAP counselling or information collected during the sessions. However, EAP counselling may be a component of a mandated employee accommodation program to, for instance, deal with an alcohol and drug abuse problem affecting the work of an employee. In such cases, it is best to make clear who the EAP and OHN professionals will be sharing information within the company, and to get the consent of the employee for this exchange of information.

Can drug and alcohol testing results be disclosed to the employer?

In some circumstances, employees are required to undergo drug and alcohol testing to meet safety standards of the position such as heavy-equipment operation or operation of large vehicles on public highways. Again, only a determination of fitness to work in relation to the safety standards should be disclosed to the employer.

Are OHNs allowed to administer random drug tests in an employment environment?

Random drug testing is a controversial surveillance practice since collection of test data is not based on probable cause, but on random selection regardless of the actions or behaviour of the worker. Generally, drug tests should be limited to pre-employment screening, post-incident investigations, or as part of a mutually agreed duty to accommodate program. All these collections of test data follow statutory requirements or case-by-case conditions.

Do I need consent of the employee to disclose health information to the Workers' Compensation Board? What about disclosure to other government officials or agencies?

The Workers' Compensation Board has legislative authority under the *Workers' Compensation Act* to collect health information from employers to process and manage a WCB claims. Therefore, the consent of the employee is not required to disclose information to the Workers' Compensation Board for this purpose so long as the information is limited to the specific injury.

Other government officials may also have legislative authority under laws such as the *Occupational Health Act* or *Public Health Act* to obtain health information without consent for certain purposes. In all such cases, the official requesting the information should identify their legislative authority and if there is any question about the release, contact the office responsible for administering access and privacy or legal counsel.

My company's privacy policy allows their lawyers to access an employee health record without consent in the case of a grievance or litigation. Doesn't this contravene OHN confidentiality guidelines?

The former CRNA Code of Ethics recognizes disclosure without consent only for emergency safety purposes or where a law requires disclosure. However, the new Code explicitly recognizes disclosure allowances set out in privacy legislation. PIPA, for

instance, allows an organization to disclose personal information without consent to legal counsel to represent the organization. The OHN should ensure, first, that the disclosure is truly necessary for the purposes of legal representation and that all other alternatives have been fully considered.

Do all occupational health professionals or those contracted to provide such services have access to all employee health information?

Occupational Health Nurses may be either employees or contracted staff. Employee health records are accessible to Occupational Health staff directly involved in the care of the specific employee.

Health professionals viewing employee health information for other purposes, such as checking the health status of their friends, family, or fellow employees, is commonly known as “snooping” and should be treated as a security breach.

Can I use fax or e-mail to transmit employee health information?

Fax and e-mail over public lines and systems is an insecure medium for transmitting employee health information - most of your breaches will occur using these devices. At the same time, the speed of these transmissions and lack of better alternatives often makes them essential to the effective and timely dissemination of health information. Take extra precautions to encrypt data transmitted over these devices and ensure that the information reaches the intended recipient.

CONCLUSION

Health care providers have traditionally been very diligent in protecting the confidentiality of their client's information. Most health professional organizations including CRNA and AOHNA have established codes of conduct and guidelines that both embrace and facilitate the practice of patient health information privacy. Regulating the protection of personal health information under law has sanctioned these traditional practices. Public and private sector health information laws in Canada recognize the significance of personal health information and require that it be managed by care providers in accordance with established legislated provisions.

Finding a balance between the need to make personal health information available and to protect it can be a challenging task. The AOHNA Privacy and Confidentiality Guidelines provide a method to assist OHN professionals in managing employee health information in the context of access and privacy legislation including collection, use and disclosure principles. It further provides guidance and interpretation of the principles of privacy legislation, securing employee health information, retention, and disposal practices and on the development of an overall privacy program.

RESOURCES

To access these resources, search them on the Internet.

Alberta Government Services

- Private Sector Privacy Resource Centre - A series of information bulletins on various issues in applying PIPA in your organization.
- FOIP Guidelines and Practices: 2009 Edition - A detailed manual on implementing FOIP in Alberta, with an index of key issues.

Canadian Nurses Association

- Code of Ethics for Registered Nurses- 2017 - The national ethics standards for all nurses in Canada, adopted by AOHNA. The Confidentiality section contains specific guidelines for protecting health privacy.
- Privacy and Health Information: Challenges for Nurses and for the Nursing Profession - An extensive discussion of the often-competing interests faced by nurses when implementing privacy in their institutions especially considering the variety and complexity of privacy laws, the challenges of electronic health records, and the need for transparency and accountability.

Office of the Information and Privacy Commissioner of Alberta

- Health Information - A Personal Matter, A Practical Guide to the Health Information Act (amended August 26, 2010) - The guide contains a detailed overview of key provisions of the Health Information Act along with practical examples for the health care setting.

Legislation

- Alberta, Health Information Act (R.S.A. 2000, c. H-5)
- Alberta, Personal Information Protection Act Regulation (S.A. 2005, c. 29)
- Alberta, Freedom of Information and Protection of Privacy Amendment Act (S.A. 2003, c. 21)
- Canada, Personal Information Protection and Electronic Documents Act (R.S.C. 2000, c. 5)
- Canada, Privacy Act (R.S.C. 1985, c. P-21)

APPENDICES

Appendix 1 - Example Excerpt from Personal Information Registry

Ref	Function / Activity	Record sSeries	Owner	Personal Information	Subjects	Security	Retention	Collection, Use Disclosure
H17	Human Resources Recruitment	Job applicants	Human Resources, Managers, Supervisors	Resume information including name, address, phone number, educational background, work background, associations and affiliations, personal achievements and specialties and any other information contained in a resume; interview notes, reference check notes correspondence, e-mails, copies of photo ID, birth date, sex, length or time at addresses, criminal history question, SIN	Employees / Applicants	Informal Office files	Current year plus 1	Owners – recruitment – implied consent
L00	Legal General	Judicial Orders	Law	Name, address, debt amounts, spouses name	Employees, Contractors, Stakeholders	Law Dept	Current year plus 6	Public
L00	Legal General	Ethics Review Results	Law	Information, evidence, and complaints concerning alleged or confirmed violationsof ethics or a conflict-of-interest policies	Employees	Stored electronically with access limited to General Counsel, Corporate Security, andtheir Administrative Support	Current year plus 6	Owner – conflict of interest, risk management -- implied consent
L02	Legal Agreements -- General	Contractors	HR, Joint Interest, Land, Sourcing	Name, Address, Banking Information, SIN or Corporate Data, references, resumes, experience records and documents, payment schedule	Contractors	Electronic Spreadsheet & hard copy Hard copies retained by & available to HR, Joint Interest, Land and Sourcing	Termination of contract plus 6 years	Owners -- Production, Revenue & Cost Allocation, Contract Administration, Contract Payments – implied consent Revenue Canada – tax purposes -- Exception

Appendix 2 - Excerpt from Privacy Impact Assessment Survey, P1 Accountability and Openness

No.	Questions	Answer	Comments (detail, rationale, changes)	Policy Reference
P1.1	Have individuals been identified who are delegated with the responsibility for privacy compliance for this project	□ Yes □ No □ N/A		PS1 4.1.1
P1.2	Have key stakeholders been provided with an opportunity to comment on the privacy protection implications of the proposed project?	□ Yes □ No □ N/A		
P1.3	Will access, privacy and security policies and practices relating to the project be made available?	□ Yes □ No □ N/A		PS1 4.8
P1.4	Have directories, registries, or records schedules, describing the content and management of the information been updated?	□ Yes □ No □ N/A		PS1 4.8 PS1 4.2
P1.5	Have communications products and/or a communications plan been developed to fully explain to the public how the personal information will be managed, including how it will be protected?	□ Yes □ No □ N/A		PS1 4.8.3
P1.6	Is any of the information transmitted across jurisdictions for the purpose of selling, leasing, or bartering the information?	□ Yes □ No □ N/A		P30(1)
P1.7	Are third parties involved in the management or use of the information?	□ Yes □ No □ N/A		PS1 4.1.3
P1.8	If yes, are there any control measures in place, including the following (check all that apply): □ an agreement that holds the third party accountable and subject to organizational privacy and security policy □ regular monitoring of the third party's compliance with organizational privacy and security policy	□ Yes □ No □ N/A		PS1 4.1.3

ACKNOWLEDGMENT

The Alberta Occupational Health Nurses Association (AOHNA) gratefully acknowledges the following individuals for their contribution to this document:

Dianne Dyck
Bev Johnston
Rick Klumpenhouwer, Cenera Consultants
Roxanne McKendry