CPTBC
College of Physical Therapists of British Columbia

Privacy Toolkit

A guide for physical therapists

updated April 2024

Acknowledgement

The College of Physical Therapists of British Columbia (CPTBC) gratefully acknowledges the Doctors of BC, the College of Physicians and Surgeons of British Columbia and the Office of the Information and Privacy Commissioner for British Columbia (OIPC) for allowing the adaptation of the *BC Physician Privacy Toolkit* to reflect the physical therapist context.

CPTBC Privacy Toolkit, First Edition - February 2020

Warning and Disclaimer

This CPTBC Privacy Toolkit has been adapted by the CPTBC and is a general guide to assist physical therapists in meeting their obligations under the *Personal Information Protection Act* (PIPA).

This Toolkit will help physical therapists to comply with the law and to meet the expectations of clients and the public in relation to health privacy. It reflects interpretations and practices regarded as valid based on available information at the time of publication.

The resource materials provided in this Toolkit are for general information purposes only. They should be adapted to the circumstances of each physical therapist using the Toolkit.

This Toolkit does not fetter or bind or constitute a decision or finding by CPTBC. It is not intended, and should not be construed, as legal or professional advice or opinion. Physical therapists concerned about the application of privacy legislation to their activities are advised to seek legal or professional advice based on their particular circumstances.

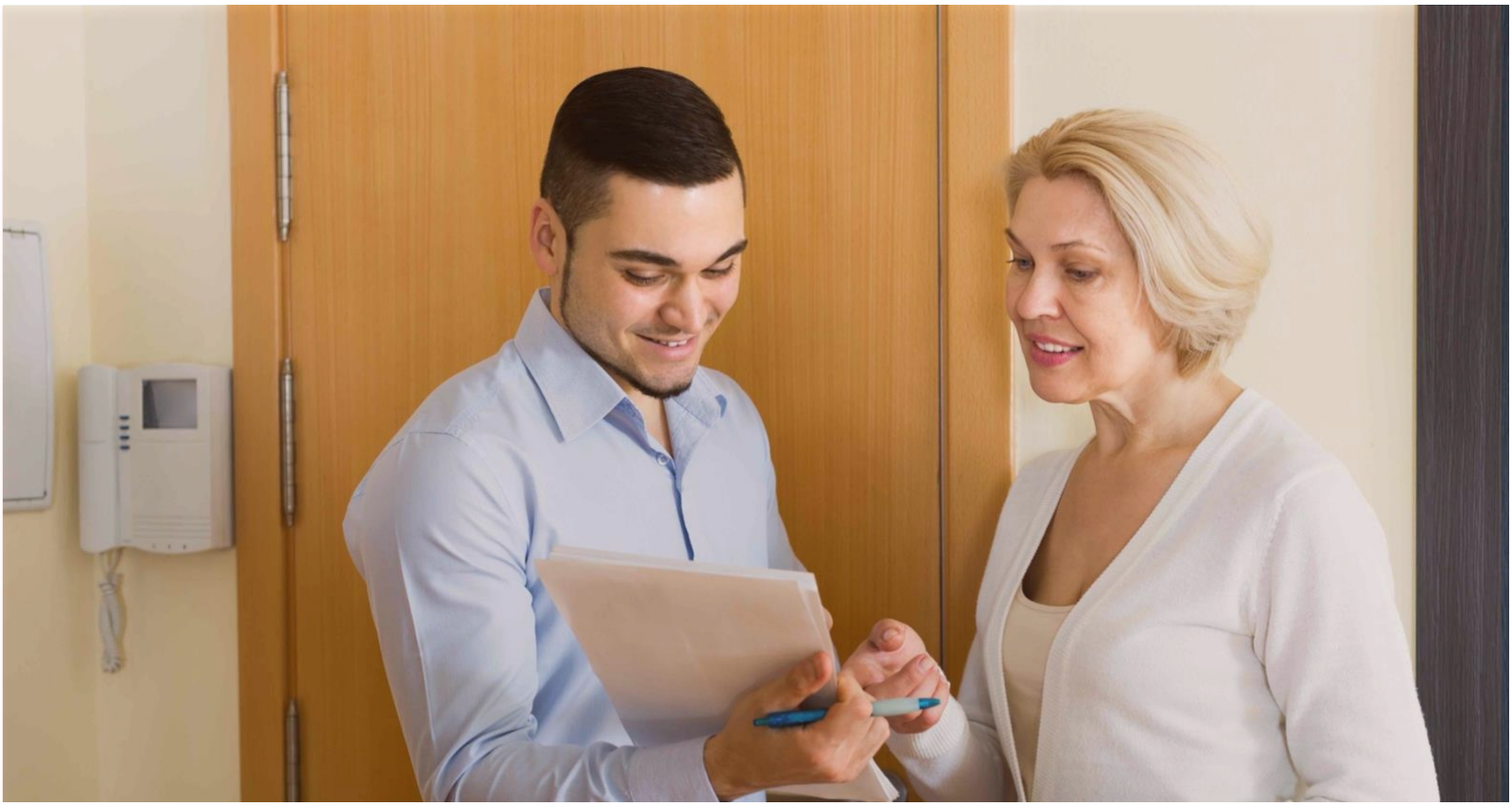
Invitation for Feedback

This is the first edition of the CPTBC Privacy Toolkit. Your feedback is always appreciated. Please contact the College with your questions or comments at *practicequestions@cptbc.org*

Contents

Click on page number to jump to it.
To return to Contents, click on the current page number or section header.

Legislative Framework for Privacy in the BC Health Care System



THIS SECTION WILL:

- ✓ SUMMARIZE THE PRIVATE SECTOR PRIVACY LEGISLATION IN BC THAT APPLIES TO PHYSICAL THERAPISTS IN PRIVATE PRACTICE AND PRIVATE HEALTH CARE ORGANIZATIONS: *PERSONAL INFORMATION PROTECTION ACT* [SBC 2003 C 63] (PIPA)
- ✓ EXPLAIN THE REQUIREMENTS OF CLIENT CONSENT AS IT RELATES TO PRIVACY
- ✓ SUMMARIZE THE PUBLIC SECTOR PRIVACY LEGISLATION IN BC THAT APPLIES TO PUBLIC BODIES, SUCH AS HEALTH CARE ORGANIZATIONS, HEALTH AUTHORITIES, PROFESSIONAL REGULATORY BODIES, MINISTRIES AND OTHER GOVERNMENT AGENCIES*: FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT* [RSBC 1996 C 165]. (FIPPA)

EXPLAIN:

- THE DIFFERENCE BETWEEN PIPA AND FIPPA
- THE ROLE OF THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF BC (OIPC)

Privacy in the BC Health Care System

Personal information related to health is one of the most sensitive types of personal information because it encompasses the physical, mental and emotional status of individuals over their lifetime. It is used for a number of purposes, including client care, financial reimbursement, education, research, social services, quality assurance, risk management, public health regulation, litigation and commerce.

Protecting clients' personal information is a priority for physical therapists because it is fundamental to maintaining the physical therapist-client relationship. When seeking physical therapy, clients disclose their personal information because they trust their physical therapist to protect their privacy. If clients do not have confidence that their physical therapist has adequate safeguards in place to protect their personal information, they may refrain from disclosing critical information, refuse to provide consent to use personal information for research purposes or not seek treatment.

Privacy and security in the health care system today must balance two competing social benefits, namely the need to appropriately access and share information to enhance care quality and safety and provide continuity of care while implementing reasonable safeguards to protect personal information.

Balancing these two needs presents challenges that can be met through a variety of measures ranging from administrative and personnel security safeguards (e.g., employee training, policies, confidentiality agreements) to technical solutions (e.g., role-based access control, auditing, authentication mechanisms, encryption). Implementing these measures will build and maintain public trust and confidence in the privacy and security of personal information.

Adequately protecting personal information is a complex undertaking within the context of requirements of privacy legislation, new information technologies (including electronic records), new models for information sharing, collaborative teams, and contractual arrangements with service providers. But none of these factors, including the introduction of new information technologies, change the responsibilities of physical therapists to appropriately protect personal information, nor do they eliminate the risks to personal information. Rather, different methods for safeguarding personal information that is stored electronically must be considered and implemented.

BC's Personal Information Protection Act (PIPA)

PIPA applies to **private organizations**, including physical therapist practices, and governs how personal information about clients, employees and volunteers may be collected, used, and disclosed.

PIPA came into force on January 1st, 2004 to govern the BC private sector – both for-profit and not-for-profit. Any organization to which PIPA applies is exempted from the federal legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which applies only to a "*federal work, undertaking, or business*" as defined in Section 1 of that Act.

PIPA does not apply to personal information collected and stored by public health care organizations such as hospitals, health authorities and the Ministry of Health. Those entities are governed by FIPPA, see below.

PIPA applies to personal information. In this context, "*personal information*" means both information that can identify an individual (e.g., name, home address, home phone number, ID numbers) and information about an identifiable individual (e.g., physical description, educational qualifications, blood type, health information). Personal information includes employee personal information, but not business contact information or work product information.

The core principle of PIPA relevant to physical therapists is that personal information should not be collected, used, or disclosed without the voluntary and informed ***consent*** of the individual.

Under PIPA, physical therapists have custody of the personal information they have collected and physical control of the documents/electronic data. They are accountable for any privacy breach that occurs to personal information in their custody and control, including any breach committed by an employee under their authority.

BC's Freedom of Information and Protection of Privacy Act (FIPPA)

In BC, public health care bodies such as hospitals, health authorities, school districts, and the Ministry of Health are subject to the privacy protective measures contained in FIPPA. FIPPA guarantees the right of individuals to gain access to and request correction of personal information collected about them by public bodies. It also prohibits the unauthorized collection, use or disclosure of personal information by public bodies and requires that reasonable safeguards be put in place to protect personal information. FIPPA does not apply to personal information collected and stored in a physical therapist's private practice or with other private health providers. PIPA governs these organizations (see above).

FIPPA prohibits the disclosure of personal information outside of Canada as well as any access to such records from outside Canada by health authorities and other public bodies without consent (except in limited circumstances). It also

provides whistle-blower protections for individuals who report contraventions of FIPPA in good faith, including unauthorized disclosure and access as well as foreign demands for disclosure or access.

FIPPA permits public bodies to provide "*foreign access*" under certain circumstances, such as performing system and equipment maintenance or data recovery from out-of-country, or with consent, and subject to other conditions. The out-of-country access must be necessary, and the information can only be accessed and stored outside of Canada for the minimum amount of time needed to complete the task.

Comparing PIPA and FIPPA

There are some notable differences between PIPA and FIPPA:

- PIPA does not restrict the storage of, or access to, personal information from outside Canada. As long as privacy is sufficiently protected, data can be stored or accessed from outside Canada.
- PIPA requires consent for the collection, use, and disclosure of personal information.
- FIPPA does not permit the collection, use and disclosure of personal information on the basis of consent to the same extent as PIPA; instead it operates on the principle of appropriate authority and "*notification*" for collection of information.

Role of the Information and Privacy Commissioner for BC

Monitoring compliance with BC privacy legislation (FIPPA and PIPA) is the responsibility of the Information and Privacy Commissioner, who is an independent officer of the BC Legislature.

If clients or employees have concerns related to privacy and security of their personal information, they can contact the OIPC for British Columbia at info@oipc.bc.ca. Also, if clients or employees are dissatisfied with how their privacy complaint was addressed by the College, they can file their complaint with the OIPC.

More information on privacy and access to information rights in British Columbia, the role of the OIPC and privacy legislation in BC can be found at *www.oipc.bc.ca*.

Ten Essential Steps for PIPA Compliance

THIS SECTION WILL IDENTIFY 10 ESSENTIAL STEPS THAT PHYSICAL THERAPISTS IN PRIVATE PRACTICE NEED TO TAKE IN ORDER TO COMPLY WITH PIPA.

THE FOLLOWING 10 STEPS SUMMARIZE THE KEY RESPONSIBILITIES THAT PHYSICAL THERAPISTS HAVE UNDER PIPA.

Step 1 – Be Accountable

Accountability in relation to privacy is the acceptance of responsibility to protect personal information. In order to demonstrate accountability and compliance with PIPA, private practices should have a comprehensive privacy management program.

Section 4(3) of PIPA states that "an organization must designate one or more individuals to be responsible for ensuring that the organization complies with this Act". The person responsible for the privacy management program is the organization's privacy officer. In a physical therapy practice, it is recommended that a physical therapist act as the privacy officer.

The privacy officer should:

- Make a personal information inventory that the practice collects (from clients, staff and contractors) and how and where it is stored.
- Make sure the practice has privacy policies and procedures that meet the obligations under PIPA and monitors compliance with them.
- Ensure all service contracts (with all contracted physical therapists, but also with accountants, bookkeepers, cleaning companies, etc.) include adequate privacy protection provisions.
- Make sure there are systems that describe how the practice will respond to access requests, requests for correction, and complaints from clients.
- Provide physical therapists and staff with mandatory privacy training and education so they know about the policies and processes, and they are familiar with PIPA's requirements.
- Use risk assessment tools to identify and mitigate any potential privacy impacts if the practice is considering new initiatives or services that involve the collection, use or disclosure of personal information.

Privacy officers may also wish to develop policies and procedures on other topics depending on the practice and the nature and volume of the personal information in its custody or control.

All components of a privacy management program should be reviewed and assessed by the privacy officer on a regular basis and revised as necessary. For example, a review might reveal that the practice needs additional security controls or improvements to privacy training and education for staff.

For further information regarding a privacy management program and the responsibilities of a privacy officer, a guidance document entitled *Getting Accountability Right with a Privacy Management Program* is available on the OIPC website.

Step 2 – Identify Purpose

PIPA provides individuals with the right to know what personal information is being collected, used or disclosed by the practice, and for what purposes. PIPA also requires that personal information only be collected for purposes that a reasonable person would consider appropriate in the circumstances. If it is not possible to identify the purpose for the collection, or if the purpose would not be appropriate to a reasonable person, the practice should not collect it. Each practice should assess its information management practices to define and document the purposes for which piece of personal information is collected, used and disclosed.

Step 3 – Obtain Consent

The core principle of PIPA relevant to physical therapists is that personal information should not be collected, used, or disclosed without the voluntary and informed ***consent*** of the individual. This principle is subject to limited exceptions which are outlined in *section 12 of PIPA*.

For example, consent is not required where the collection, use, and disclosure of personal information are:

- clearly in the interests of the individual and consent cannot be obtained in a timely way, or
- necessary for medical treatment of the individual and the individual is either unable to give consent or does not have the legal capacity to give consent

Consent is indicated by the individual willingly agreeing to the collection, use, and disclosure of personal information for a defined purpose. Consent can be given verbally or in writing, but consent in writing may provide stronger evidence that consent was given if that is later challenged.

Section 8 of PIPA describes where implicit consent can be relied upon. This includes where the collection, use or disclosure of personal information:

- is for a purpose that would be considered obvious to a reasonable person, and
- the individual voluntarily provides the personal information for that purpose

Where relying on implicit consent, it must still be informed consent, and the physical therapist must:

- advise the client, in plain language, how their personal information will be used and disclosed, and
- give them a reasonable opportunity to decline, and
- ensure the use and disclosure is reasonable, considering the sensitivity of the personal information in the circumstances

A client has the right to withdraw their consent to further collection, use or disclosure of their personal information at any time without retribution.

College Standard of Practice Privacy and Record Retention - requires that the physical therapist obtains and documents clients' informed consent prior to disclosing personal information to other parties, including communicating and sharing information electronically.

ICBC clients should be informed at the initiation of physical therapy services that Section 28 of the *Insurance Vehicle Act* allows ICBC to request reports, and that the physical therapist is obliged to provide these reports. If the client does not consent to the requested reports being sent to ICBC they should be asked to communicate with ICBC or their lawyer for clarification and to then direct the physical therapist about how to proceed. It is best to advise clients **prior to** the delivery of physical therapy services of this obligation to provide requested reports. If a physical therapist wishes to send a report to ICBC that was not requested by the insurer under Section 28 then client consent must be obtained.

Step 4 – Limit Collection

A practice should collect only the minimum amount of personal information that is necessary to achieve the purpose of the collection.

Step 5 – Limit Use, Disclosure, Storage and Retention

A practice must use and disclose personal information in accordance with the purpose(s) of collection. Consent is required for use and disclosure of personal information for new purposes, unless it is otherwise authorized by PIPA as described above in Step 3. Information should be kept only for as long as necessary to meet the original purposes or as required by the CPTBC Bylaws and Standards of Practice. CPTBC Standards require that clinical records be retained for at least 16 years from the date of last entry, or in the case of a minor, 16 years from the age of majority (19 years of age). Records containing personal information (whether paper or electronic) should be disposed of appropriately, safely, and definitively when they are no longer required. For more information, see *Bylaw 84: Registrant Records* and *Standard of Practice: Documentation*.

Step 6 – Maintain Accuracy

Physical therapists must ensure that clinical records are complete and accurate. The privacy officer should develop procedures that will ensure information is collected and maintained accurately. For example:

- forms can be used to ensure all necessary personal information is collected
- questions can be asked at each client visit to confirm certain personal information that might have changed between visits

Under PIPA, individuals have the right to request that their personal information be corrected if they believe it is not accurate or complete. This right applies to correcting factual errors or omissions in their personal information and does not apply to professional/clinical opinions. Individuals (or their legally authorized representative) may make a request

for correction in writing (see form – *Correcting Personal Information*) and a practice must respond within 30 working days of receiving a request.

In order to make the correction, the physical therapist or practice must be satisfied on reasonable grounds that the correction should be made. If a correction is made, a copy of the amendment must be sent to each individual or organization to which the inaccurate or incomplete information was disclosed within the past year. If no correction is made, the practice is required to annotate the information with the correction that was requested but denied, and the reasons for not making the correction must be provided to the requesting individual. Requests for corrections to professional reports or expert opinions are usually annotated.

The privacy officer must educate staff on how to appropriately respond to such requests. If a client is not satisfied with the outcome, they may take the matter to the OIPC and/or make a complaint to CPTBC.

Step 7 – Employ Safeguards

A practice must implement reasonable security safeguards to protect personal information against loss, theft or other unauthorized access, use or disclosure. Safeguards refer to administrative, physical and technical measures, and may include a combination of policies, practices and software that protect personal information. The sensitivity of the personal information informs what types of safeguards are appropriate in the circumstances, irrespective of the form in which a clinical record is stored (paper, electronic, digital). Clinical records must be handled in a secure manner from the time the records are created to the time they are disposed of, regardless of the format in which the information is stored.

The following are best practices in safeguarding clinical records and other personal information stored by the practice. Note that a combination of measures may be required during the transition from paper-based clinical records to electronic records where both methods of record-keeping may be used in parallel.

In order to protect clinical records, it is recommended that staff:

- wear building passes/photo ID (if issued)
- verify that persons who don't look familiar have a legitimate reason to be there
- know how to respond if suspicious behaviours are noticed
- not disclose confidential information about how the practice's security systems operate
- sign confidentiality agreements that specify obligations and expectations including consequences for inappropriately collecting, using or disclosing personal information

Paper records should be:

- retrieved promptly from fax machines or photocopiers
- clearly labelled
- placed in a location that prevents members of the public from viewing the records (e.g., avoid leaving clinical records at the reception desk where other clients can see them)
- returned to the filing location as soon as possible after use
- stored:
    - on-site wherever possible
    - securely within the practice (e.g. in locked cabinets)
    - in a location where members of the public cannot access the contents
    - tracked if being transferred by confirming that the records have arrived at their specified destination
    - kept secure at all times if taken off-site

In order to protect personal information stored in electronic records, staff should:

- log out of computer systems or applications when unattended or not in use
- keep workstations positioned away from public view and access
- memorize or use a secure password manager instead of writing down passwords
- not share an assigned user ID and password with others

The privacy officer should also do the following to protect personal information stored in electronic records:

- create a unique user ID and strong password for every authorized user, including student physical therapists
- grant role-based access to staff working in the practice on an individual basis based on a “need to know” and “least privilege” principles
- revoke user IDs and passwords as soon as authorized users resign or are dismissed
- install strong, up-to-date, industry-standard encryption
- implement password changes forced at regular intervals
- install firewall software and regularly update internet-based computer systems
- create audit trails to track when a client record is accessed and by whom, including date and time
- activate password protected screensavers or auto log out for computers after a period of inactivity to avoid unauthorized viewing
- consider installing a privacy screen filter to prevent viewing of the screen from an angle
- verify that data backup methods and disaster recovery plans are in place and are periodically reviewed and tested

Note: CPTBC occasionally hears from physical therapists who need advice after a computer glitch when they discover their backup hasn't happened for some time or that the backup files are unreadable. It is important to periodically review backup data to ensure that the backup is occurring as scheduled and that records are accessible if needed.

Step 8 – Be Transparent

A practice should be transparent about its information management policies and procedures and provide this information to individuals upon request. This includes providing information to clients and employees about what personal information the practice collects, the purposes for which the information is used, to whom it is disclosed, how it is protected, and how an individual may access or correct their own personal information. This can be achieved through client handouts or posted notices.

Step 9 – Provide Access

Clients and employees are entitled to access their personal information that is in the custody or control of the practice. According to Section 32 of *PIPA* a physical therapist may charge "a minimal fee for access", unless the information is that person's employee personal information. For more information, see form *Request for Access to Personal Information*.

The privacy officer should develop procedures that allow a person to have access to their own records. The process should allow both clients and employees to access and request correction of their personal information. These procedures should set out what minimal fees will be charged for client access to records. The minimal fee is intended to recover some of the actual and necessary costs incurred by the practice to provide access, and may include the costs associated with locating, retrieving, producing and copying a record, preparing the record for disclosure and any postage or shipping costs. The minimal fee may include the cost of reviewing the records prior to their disclosure both for information that is not part of the access request, or for information that should be withheld.

Information that should be withheld includes:

- personal information of other individuals
- information that could reasonably be expected to threaten the safety, physical or mental health of a third party
- information that could cause immediate or grave harm to the individual who made the request
- information that is subject to solicitor-client privilege

When charging fees, the practice must provide the applicant with a written estimate of the total fee, and may require the applicant to pay a deposit for all or part of the fee before processing the request.

Step 10 – Permit Recourse

Individuals, including clients and employees, have the right to challenge a practice's compliance with PIPA. PIPA requires a practice to develop a process to respond to such complaints. If the individual who made the complaint is not satisfied with the practice's response, they have the right to make a *complaint to CPTBC* and/or to the OIPC at *www.oipc.bc.ca*. Resolving complaints through the practice's privacy officer can be a more efficient way to address client or employee concerns relating to privacy and access to information issues.

Guidelines for Confidentiality Agreements and Service Contracts

THIS SECTION WILL IDENTIFY:

- ✓ KEY ELEMENTS TO INCLUDE IN CONFIDENTIALITY AGREEMENTS
- ✓ KEY PRIVACY-PROTECTIVE ELEMENTS TO INCLUDE IN SERVICE CONTRACTS

Service providers, suppliers, partners, employees, and others may be engaged by physical therapists to assist them in their practice. During their work, these third-party individuals or organizations are likely to be exposed to personal information in the custody and control of the practice. Therefore, depending on the situation, privacy-protective contractual clauses and confidentiality agreements should be in place to ensure that third parties comply with the practice's expectations that personal information will be appropriately safeguarded in compliance with PIPA. If third parties must collect, use or disclose personal information as part of their contractual obligations, it's important to ensure they have the legal authority to do so.

Confidentiality Agreements

A physical therapist's obligation to safeguard personal information means having internal staff and third parties who have access to personal information sign a confidentiality agreement. Some of the elements to be included in a confidentiality agreement include:

- establishing what personal information must be kept confidential and what security safeguards are required,
- clarifying who has custody and control of the personal information, and
- what the consequences are for non-compliance with the agreement.

These sample confidentiality agreements may be used as a guide:

- *Confidentiality Agreement for Employees*
- *Confidentiality Agreement for Third Parties*

Privacy Considerations in Service Contracts

Before entering into a service contract with an external service provider (e.g., application service provider, electronic record vendor, record destruction services, storage retrieval services, bookkeeper/accountant, translator), physical therapists can protect personal information by ensuring:

- service providers have effective and comprehensive information management practices that are at least equal to those implemented by the practice
- contracts include the appropriate security arrangements and privacy protection clauses

These requirements should be monitored and enforced by the service provider. For service providers that frequently handle sensitive personal information as part of the contract, the practice should undertake audits to verify compliance.

When preparing a contract with a service provider, the following elements may be included:

- Identification of:
    - all applicable privacy laws and a clear statement that the service provider must comply with these as well as their own privacy laws and policies
    - the purposes for which the personal information can be collected, used, or disclosed based on the client's initial consent and restrictions on any further use to those purposes, except as permitted or required by law
    - who will maintain custody or control of the personal information, and how access will be granted in the event that a service provider changes in future (for example electronic record providers).
- A requirement that service providers:
    - only collect, use, access and retain the information provided to them as identified in the contract
    - only allow access to subcontractors after the practice is made aware of it and has approved their access
    - allow the practice to access its information upon request and never deny access because of a disputed payment for services. This is especially important for electronic record service providers (see below) as physical therapists are obliged to retain clinical records and to allow client access when requested.
    - notify the practice if any personal information has been lost, stolen, used, or accessed in an unauthorized manner
    - report any privacy breach or security incident within an agreed-upon timeframe
    - return or destroy personal information when the contract ends as specified

In particular, when preparing a contract with an electronic record service provider, include:

- all reasonable physical, administrative and technical safeguards to protect the personal information from unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks
- any financial or other consequences that may result from non-compliance with the contract
- enduring access to clinical records in the event that a practice changes electronic record providers. The contract should require the electronic record provider to:
    - make the data available in a portable format,
    - transfer the data to another electronic record or disclose it within a certain number of days; and

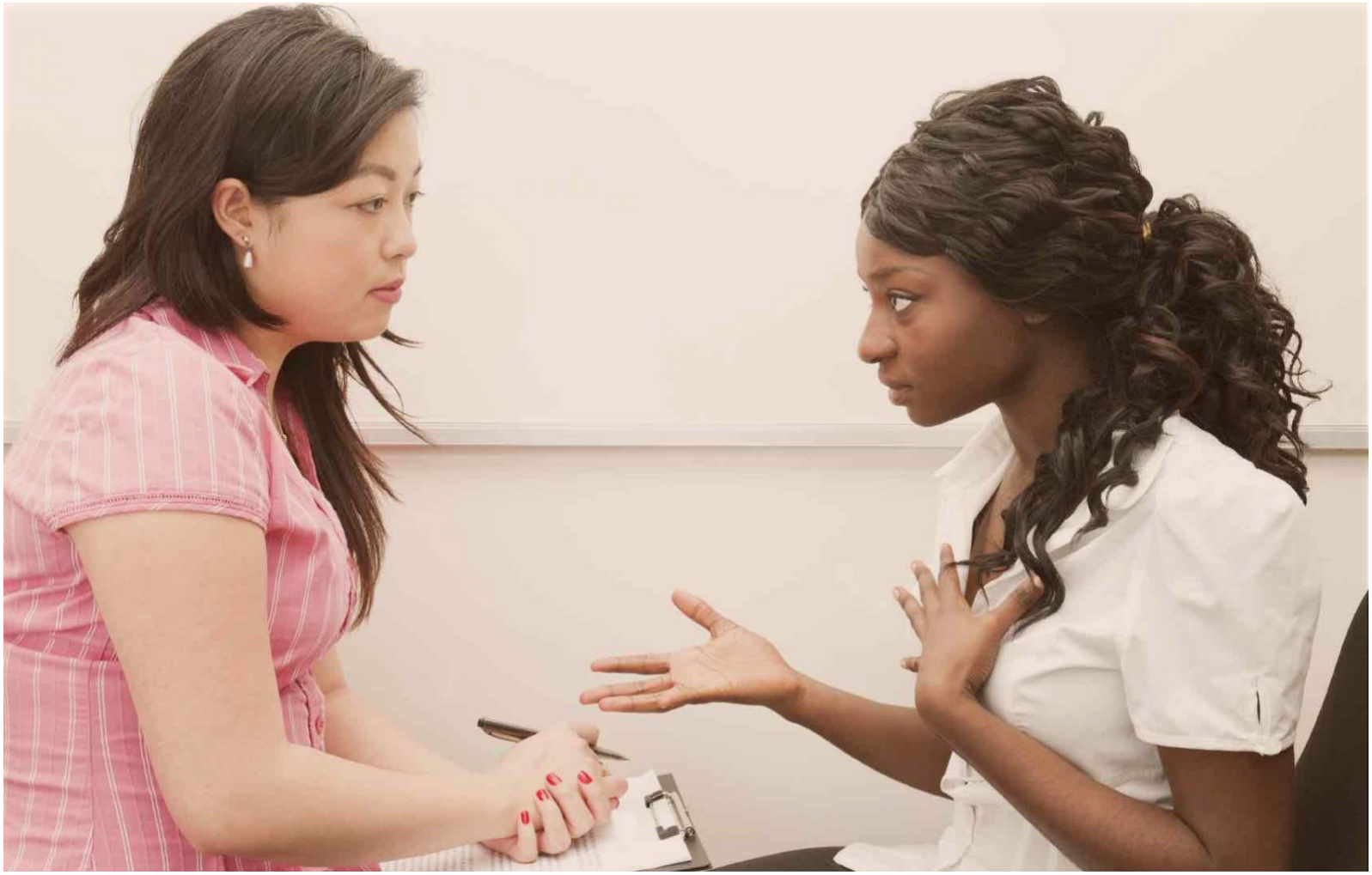
- destroy their own copy of the data after it has been successfully transferred.

See also page 27 for more information about electronic records and privacy considerations

Many service providers do operate some or all portions of their services out-of-country for a variety of reasons. In these circumstances, the contract should specify:

- where personal information is being stored, who has access, and what security provisions are in place
- in situations where there are remote access capabilities, from what locations personal information may be accessed
- for any aspect of the service provider's operations that are out-of-country, the contract binds the service provider to PIPA, as their own jurisdiction may not have any or adequate privacy laws, compared to BC standards

Guidelines for Consent and Masking Options



THIS SECTION WILL:

- ✓ DEFINE PHYSICAL THERAPIST RESPONSIBILITIES REGARDING A CLIENT'S CONSENT FOR THE COLLECTION, USE, AND DISCLOSURE OF THEIR PERSONAL INFORMATION
- ✓ DISCUSS MASKING OPTIONS AND PHYSICAL THERAPIST RESPONSIBILITIES IN ELECTRONIC RECORDS WHEN PERSONAL INFORMATION IS MASKED

Consent

Consent is a person's verbal or written agreement to the collection, use and disclosure of their personal information for a defined purpose. PIPA includes a provision for implicit consent which may be relied upon if specific conditions are met:

Implicit consent:

- must be voluntary and informed, and physical therapists have a responsibility to provide adequate information to clients on how the practice manages personal information,
- may be established when an individual is provided with notice about the collection, use, and disclosure of personal information in a form they can reasonably understand and for reasonable purposes given the sensitivity of the personal information, and
- is established after the individual is provided with a reasonable opportunity to decline

For consent to be meaningful, the individual has to know that they have the right to withhold or withdraw consent at any time without fear of retribution.

Masking Options (Disclosure Directives)

Clients may have the option to restrict access to certain personal information about them that is stored in electronic records systems. This privacy protective feature of an electronic record system is known as "masking", and clients should be informed of this right.

Many electronic records applications have explored and implemented "masking" options. The ability to mask is often considered when a single electronic record application is shared in a multidisciplinary or group practice setting. This provides clients with the ability to control who in the group may or may not have access to some or all of their personal information.

Physical therapists should inform clients about the option to mask personal information in their record, as well as the effects of "masking" on delivery of care.

If a competent client decides to mask their record such that some information is hidden from the physical therapist, the physical therapist must:

- honour the client's decision and only access the personal information with consent
- document in the client's clinical record the discussion and the client's decision
- provide the best care possible working with the information at their disposal

In some cases a physical therapist may determine that it is unsafe to treat a client without having access to relevant health information. A physical therapist who is treating a client whose information has been masked, and who does not give the physical therapist consent to access, has an obligation to obtain a history from the client prior to determining whether or not to proceed with treatment. Taking a proper history may elicit relevant information, and resolve the physical therapist's concerns of not being able to access masked information. When a client refuses to discuss relevant information, this refusal should also be documented.

If the inability to access masked information creates a situation where the physical therapist feels there is a safety risk, the physical therapist can refuse to provide treatment. The physical therapist should explain the reasons for their decision not to treat the client and note all relevant discussions in the client's clinical record.

Guidelines for Electronic Records and Role-Based Access

THIS SECTION WILL:

- ✓ SUMMARIZE PRIVACY AND SECURITY CONSIDERATIONS DURING THE TRANSITION FROM PAPER TO ELECTRONIC RECORDS
- ✓ DEFINE ROLE-BASED ACCESS AND IDENTIFY KEY CONSIDERATIONS RELATED TO ELECTRONIC RECORD IMPLEMENTATION
- ✓ IDENTIFY PRIVACY AND SECURITY BEST PRACTICES

Making the Transition to Electronic Records

Physical therapists practise in a context where they are required to adhere to documentation practice standards and are responsible for their client records, whether they are in paper or electronic form.

The transition from a traditional paper-based client record to an electronic system that uses new technologies is a significant undertaking, requiring changes to a practice from many perspectives – clinically, administratively, and organizationally. Physical therapists must be prepared to maintain the protection of personal information during the transition period where both paper and electronic versions exist in parallel.

During the transition to electronic records, the following recommended steps may be of assistance:

- understand existing paper-based workflow processes and integrate them into the use of electronic records to achieve the greatest benefits
- revise existing privacy and security policies and practices to reflect the use of electronic records and personal information in electronic format
- update staff privacy training to incorporate an understanding of the changes associated with electronic records
- retain the original medical record and once the information has been fully transitioned to an electronic record, dispose of it securely
- if only part of the paper record is transitioned to an electronic record, retain the remainder of the paper record as part of the original medical record
- save scanned copies of paper records in “read-only” format so they cannot be altered
- if using optical character recognition (OCR) technology to convert records into searchable and editable files, retain either the original record or a scanned copy to ensure accuracy
- ensure clients still have access to their complete information upon request, even if the information now exists in a combination of formats (paper, electronic, digital)

Role-Based Access

Role-based access to electronic records is essential. Role-based access uses information technology to protect the personal information of the client by ensuring that access to that information is based on the "need to know" and "least privilege" principles.

The role-based access model identifies all possible roles in an organization or practice that require access to a client's personal information, and assigns each of these roles access to only the type and amount of personal information needed to perform the job function. For example, specific permissions (e.g., reading, writing, printing) can be assigned to certain personal information based on the job duties of the person who has access.

Roles can be defined for all of the various users, whether they are employees or otherwise, who access the electronic record. These include clerical staff, billing services, students, physical therapist support workers, locum physical therapists, and other physical therapists within the practice. When assigning a role, a prudent physical therapist will always assess the degree to which access to the client's personal information is truly necessary for that person to perform their duties.

Implementing this model also allows for ease of account management when setting up new users and modifying accounts. Role-based access models must be designed to support both business and clinical workflow, and as such the electronic record software must have flexibility to support the unique needs of each practice. It must also allow for exceptions to the standard role and permissions, provided it is authorized and necessary for the performance of job duties.

An authorized role alone does not entitle an individual to access a given record, as the individual must also have a "need to know" based on their provision of care to the client. "Need to know" can frequently become "want to know", which may not meet the required threshold for granting authorized access or may lead to workplace snooping.

When determining which functional areas and permissions should be assigned to each role and user, ask:

- Can existing users currently access all of this information?
- Does each of these roles truly need access to all areas of available information?
- Are the users unable to carry out the requirements of their job if they do not have access to this information?
- Can the client suffer harm if the user does not have access to this information?
- Is the information required to support the care of the client across the continuum of care?
- Does the user require regular and routine access to this information or do they only require access on an occasional basis where other methods of access may suffice?

When defining roles, assigning access and granting permissions associated with each role, ask:

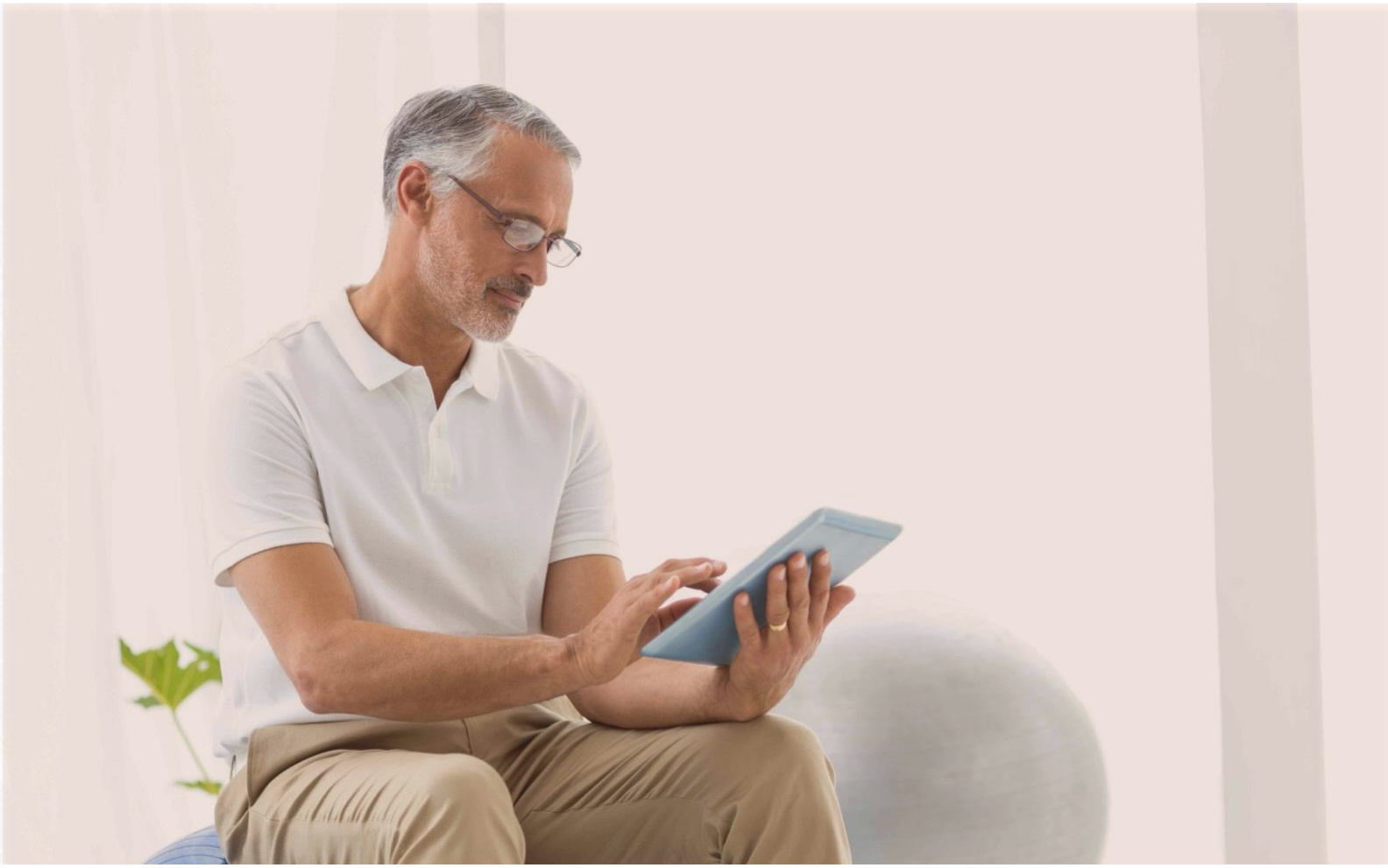
- What are all the possible roles that would require access to personal information in the practice?
- What are the possible functional areas when that information may need to be accessed (e.g., clerical, clinical, financial/billing)?
- What are all the possible permissions that could be assigned to each role (e.g., create, read only, update, delete)?
- Are there additional permissions that a user in a role could be assigned (e.g., mask/unmask information, print, email)?

Privacy and Security Considerations

Physical therapists are responsible for data stewardship, and assume responsibility for any access to personal information, including by staff and contractors. To be effective as a privacy-enhancing mechanism, role-based access should be used in conjunction with additional privacy and security controls, such as:

- automatic log off feature
- strong, up-to-date, industry-standard encryption applied to electronic record data and portable electronic devices
- audit trails to record user access
- allowance for correction/annotation of information
- ability to mask/unmask sensitive data
- unique user IDs and passwords, including for students
- not granting access until the user is authorized by a physical therapist, has completed training, is provided with privacy education, has signed a confidentiality agreement and is made aware of practice privacy and confidentiality policies
- ensuring that audit log capability is activated in the electronic record system to track all user access to client information for the purposes of compliance monitoring and incident investigation
- managing user accounts including adding, modifying, and de-activating user accounts on a regular and timely basis
- confidentiality disclaimers on printed reports
- robust backup and recovery procedures

Guidelines for Ensuring Accuracy of Clinical Records and Responding to Client Correction Requests



THIS SECTION WILL:

- ✓ EXPLAIN CLIENTS' RIGHTS TO VERIFY THE ACCURACY OF THEIR CLINICAL RECORDS AND ASK FOR CORRECTIONS
- ✓ IDENTIFY REQUIREMENTS TO KEEP PAPER AND ELECTRONIC RECORDS ACCURATE

Personal information must be documented in the record as soon as possible, providing current information on the assessment and treatment of the client. The clinical consequences of inaccurate personal information can range from personal embarrassment to physical harm or even death in extreme cases.

Because individuals have the right to request corrections to their personal information if they believe it is not accurate or complete, a practice's privacy policy should describe how personal information is kept accurate and how clients may request corrections to their information. Clients (or their legally authorized representative) may make a request for correction in writing (see form – *Correcting Personal Information*) and a practice must respond **within 30 working days** of receiving a request. The privacy officer should ensure the staff know how to respond appropriately to these requests.

Best practices for maintaining accuracy include that personal information in **paper-based medical records** should be:

- written clearly, legibly, and in such a manner that it cannot be erased
- readable on any photocopies or faxes
- accurately dated and signed, with the name of the author printed alongside the first entry
- wherever possible, written with the involvement of the client
- clear, unambiguous, and with abbreviations, if used, that follow common conventions
- for any alterations or additions, dated and signed in such a way that the original entry can still be read clearly
- when not making a requested correction, noted clearly with details of the request and reasons for not making changes
- organized in a consecutive or chronological order

Additional information must also be included in accordance with *College Standard of Practice: Documentation*.

Best practices for maintaining accuracy include that personal information in electronic records should be maintained in electronic records that:

- have the ability to correct information through an amendment (e.g., the original data must not be modified or deleted as history should be maintained)
- accurately date and time-stamp a correction, recording who made the amendment
- allow for an annotation whenever a correction is requested but not made
- can generate a copy of a clinical record with the amended information and correction history

Guidelines for Photography, Videotaping, and Other Imaging

THIS SECTION WILL:

- ✓ DESCRIBE REASONABLE PRACTICES FOR PROTECTING PERSONAL INFORMATION WHEN USING PHOTOGRAPHY, VIDEOTAPE, DIGITAL IMAGING, OR OTHER VISUAL RECORDINGS
- ✓ IDENTIFY WHAT NEEDS TO BE DONE BEFORE, DURING, AND AFTER PHOTOGRAPHING OR RECORDING CLIENTS

These guidelines should be followed when using photography, videotape, digital imaging, or other visual recordings, for the purpose of providing care to a client, for education, or for research.

If photographs or videotape recordings that identify clients are required for the purpose of providing care, the physical therapist should obtain written consent from the client. This consent does not authorize the collection, use or disclosure of the images for any other purposes such as education, scientific publication or research, or use on social media unless these purposes are expressly stated in the consent form.

Before photographing or recording clients, physical therapists are required to:

- Obtain consent:
  - from clients for the collection, use and disclosure of photographs or recordings
  - although verbal consent is sufficient, best practices include that the client is provided with a written consent form that provides relevant information (including the purposes for collection, use and disclosure) in a way that the client can understand (translations should be provided where necessary prior to signing the form), and the client is given a reasonable amount of time to consider the information.
  - from a parent or guardian if the client is a child who is incapable of exercising their legal rights
  - from a personal representative if a client is deemed incapable or incompetent
  - for any use or disclosure beyond the original purpose
- Ensure the client understands:
  - the purpose for which the photograph or recording is taken and how it will be used
  - who will be allowed access to it
  - whether copies will be made
  - how long the photograph or recording will be kept, and how it will be stored

- Inform the client that:
    - refusal to consent will not affect the quality of care being offered
    - their consent can be withdrawn at any time without consequence
- Immediately stop the photography or recording session if the client withdraws consent

After the photography or recording session, best practices dictate that physical therapists are responsible for:

- ensuring all photographs, videotapes, recordings or images are identified with the client's name or unique identifier, and date
- ensuring the photograph or recording is securely destroyed or erased as soon as possible if the client withdraws consent
- storing photographs, videotapes or recordings with the client's clinical record or if stored separately in a secure area, noting the location of the photos, recordings, or images in the client's clinical record
- ensuring the same level of security over photographs, videotapes, recordings or images as for all confidential clinical records

Where photographs, videotapes, recordings, or images may be shown to third parties, consent is necessary, except where required by law. The client should be:

- made aware of and understand that the photographs or recordings may be shown to people who may not have any responsibility for their health care
- made aware of the right to request their personal information, including photographs or recordings, in the form in which they are intended to be shown, and
- have the right to withdraw consent

No photograph or recording should be made contrary to the client's wishes.

In exceptional circumstances, the photograph or recording may be captured without the client's consent. An example of this circumstance is if the client's consent for capturing a photograph or recording cannot be obtained in a timely way or the client is unable to give consent, and the collection of this personal information is clearly in the interest of the individual or is necessary for the client's treatment. The physical therapist must subsequently request the client's consent prior to disclosing the photograph or recording for use beyond the client's immediate care needs.

Guidelines for Protecting Clinical Records When CLOSING a Practice

THIS SECTION WILL:

- ✓ DESCRIBE BEST PRACTICES REGARDING CLINICAL RECORDS WHEN CLOSING A PRACTICE
- ✓ IDENTIFY KEY CONSIDERATIONS AND ELEMENTS OF CONTRACTS WITH A SERVICE PROVIDER TO PROVIDE STORAGE, RETRIEVAL, OR DESTRUCTION OF CLINICAL RECORDS

When a physical therapy practice is closed, replaced, or relocated outside of BC, physical therapists have a professional and legal duty to use reasonable efforts to do the following with clinical records:

- Arrange secure transfer to another physical therapist who agrees to accept responsibility for the records, or
- Arrange for secure storage and retrieval for the remaining retention periods.
- Securely dispose of clinical records where the retention period has expired.
- College Bylaws also allow the option of returning the record to the person the information pertains to. Legal advice may be helpful if considering this option.

College Bylaw 86 (5)(b) requires the physical therapist to notify the College in writing within 21 days of the steps taken to transfer or store the personal information. There is a *notification form available* on the CPTBC website to complete and submit to the College.

Physical therapists must ensure that whoever accepts responsibility for custody of clinical records understands where those clinical records are being stored and who can have access to them. The records must be stored safely and securely and accessible when necessary.

If a service provider is engaged to provide storage and retrieval services for clinical records for the remaining retention period, physical therapists should ensure this is done under a service contract that places the following kinds of obligations on the service provider:

- Maintain the confidentiality of all clinical records stored, providing access to information only to authorized representatives of the physical therapist or with written authorization from a client or legal representative.
- Upon request of the physical therapist, promptly return all confidential clinical records without retaining copies.
- Prohibit the use of clinical records for any purpose other than what was mutually agreed upon (this prohibits selling, sharing, discussing or transferring any clinical records to unauthorized business entities, organizations, or individuals).
- Use reasonable administrative, physical and technical safeguards to protect against theft, loss, damage, and unauthorized access of clinical records.
- As specified by the physical therapist, securely destroy clinical records at the end of the retention period in accordance with College Bylaw 86(5)(a)(iii).

Guidelines for Protecting Clinical Records Outside the Practice

THIS SECTION WILL:

- ✓ **IDENTIFY BEST PRACTICES FOR PROTECTING PAPER AND ELECTRONIC CLINICAL RECORDS WHEN OUTSIDE OF THE CLINIC**

Physical therapists have a legal and ethical obligation to respect client confidentiality and to protect personal information. The College Code of Ethical Conduct requires physical therapists to protect the personal information of their clients. PIPA requires that physical therapists take reasonable measures to protect clients' personal information from risks of unauthorized access, use, disclosure and disposal and sets out consequences for violation. The OIPC has described reasonableness as the measure by which security measures are objectively diligent and prudent in the circumstance and stated that what is 'reasonable' may signify a very high level of rigour depending on the situation.

Protecting Clinical Records Outside the Practice

There are times when physical therapists and their staff may need to access personal information remotely while travelling, at home or in another location. This includes transporting records by car or airplane, working from home, attending meetings or conferences or making visits to a client's home. The personal information may be stored in paper records or on portable electronic devices such as laptops, external hard drives, USB storage devices, handheld electronic devices and smart phones. With electronic records and other forms of electronic communication, physical therapists and their staff are also able to connect to their practice network and may have access to sensitive personal information from anywhere in the world.

Physical therapists must implement reasonable safeguards, including administrative, physical and technical measures, to reduce the privacy risks of accessing personal information outside the practice.

Conversations

When having conversations outside the practice, physical therapists and staff should:

- Avoid discussing a client's personal information in public areas such as on elevators, in stairwells, while travelling by public transit or airplanes, in restaurants or on the street.
- Avoid using cell phones to discuss a client's personal information while in transit as these conversations can be intercepted or overheard.
- Use a password protected voicemail when working from home.

Paper Clinical Records

When using paper clinical records, physical therapists and staff should:

- only remove clinical records from the practice when it is absolutely necessary for performing job duties
- require all staff to obtain approval from their supervisor before removing clinical records from the practice
- use a sign-out sheet to document who is removing a clinical record, the name of the individual whose personal information is being removed, and the date the record is being removed
- leave the originals in the practice, where possible
- take only the minimum amount of personal information required to perform the task
- if the records are large, consider using a courier to transport them to their destination
- place records in confidential folders, transport them in a secure manner, and keep them under control at all times, including meal and break times
- keep records locked in a desk drawer or filing cabinet when working from home to reduce unauthorized viewing and access by family members or friends
- if transporting clinical records by car, keep them locked in the trunk before the start of the trip
- never leave clinical records unattended while in transit, even if they are stored in the trunk as these are still accessible to thieves
- never examine clinical records in public places where they may be viewed or accessed by unauthorized individuals (e.g., on public transit)
- never leave clinical records open for view in hotel rooms (e.g., keep them in the hotel safe)
- immediately return clinical records to their original storage location upon returning to the practice
- securely destroy any copies that are no longer required

Portable Devices

PIPA requires that any personal information stored on a portable electronic device be protected by industry-standard encryption. When accessing clinical records on portable electronic devices, physical therapists and staff should:

- avoid storing personal information on portable electronic devices unless absolutely necessary
- protect wireless transfer of personal information or storage on cloud-based programs with industry-standard encryption
- protect portable electronic devices containing personal information with a strong password and use a secure method, such as two-factor authentication, to grant user access
- keep portable electronic devices secure to prevent loss or theft (e.g., in a locked briefcase, desk drawer, container or room) and keep them under one person's control at all times, including meal and break times

- if transporting portable electronic devices by car, keep them with the physical therapist at all times or lock them in the car trunk before the start of a car trip
- never leave portable electronic devices unattended, even if stored in the trunk
- remove all sensitive personal information when no longer needed from portable electronic devices using a digital wipe utility program (do not rely on the delete function as the information may still remain on the device)

Electronic Records

When accessing clinical records on home computers/laptops or portable electronic devices, physical therapists and staff should assess the security risks and consider the following:

- never use public computers or public wireless networks to connect to the practice network as these are not secure
- require a password protected login to access personal information and avoid recording passwords or allowing your device to save them
- use encrypted email transmissions and ensure that personal email has proper access control. For more information about E-mail security see section 11 of the OIPC document *Securing Personal Information: A Self-Assessment Tool for Organizations*
- log off from a home computer when not in use
- set an automatic log out to occur after a period of inactivity
- depending on the security risks of the physical environment, lock laptop computers that are used for work-related purposes to a table or other stationary object with a security cable, or keep home computers in a room with restricted access
- use strong, up-to-date, industry-standard encryption and password protection for any personal information that must be stored on hard drives
- ensure that home computers have, at a minimum, a personal firewall, anti-virus protection, and anti-spyware protection
- ensure the latest updates and security patches are regularly installed
- use an encrypted link to the host network, such as a virtual private network (VPN), when accessing personal information remotely
- watch out for “shoulder-surfing” where family members or friends may casually observe the screen of the home computer

Guidelines for Providing Tele-rehabilitation Security Safeguards

Security Safeguards

It is essential that physical therapists ensure tele-rehabilitation systems have appropriate security measures and are otherwise PIPA compliant. For example, physical therapists should only use systems with up-to-date, industry-standard encryption for transmission of data. To reduce the amount of personal information disclosed to companies providing tele-rehabilitation, physical therapists should try to communicate with each other about clients without referring to the client's unique identifiers, where feasible.

Guidelines for Responding to a Privacy Breach

THIS SECTION WILL:

- ✓ EXPLAIN WHAT CONSTITUTES A PRIVACY BREACH
- ✓ IDENTIFY WHISTLE-BLOWER PROTECTIONS IN PIPA
- ✓ EXPLAIN THE ROLE OF OIPC WITH REGARD TO BREACHES
- ✓ IDENTIFY THE FOUR ACTIONS THAT PHYSICAL THERAPISTS NEED TO TAKE FOLLOWING A SUSPECTED OR CONFIRMED BREACH

PIPA requires physical therapists to protect personal information that is under their custody and control. Part of that responsibility involves managing privacy breaches, including taking steps to prevent them from occurring, developing a privacy breach response plan and promptly responding when a breach occurs. A privacy breach occurs when there is unauthorized collection, use, disclosure, retention, or disposal of personal information. Those activities are "unauthorized" if they occur in contravention of PIPA.

The following scenarios are common examples of how a privacy breach can occur.

- Personal information is stolen or misplaced.
- A client's clinical record or an electronic portable device containing personal information (e.g., laptop, handheld electronic device, USB storage device) is lost or stolen.
- A letter containing a client's personal information is inadvertently sent by mail, fax or electronically to an incorrect address or to the wrong person.
- A clinical record is saved in a web folder that is publicly accessible online.
- A physical therapist sells a computer previously used by the practice without first deleting the personal information saved on the computer and securely wiping the hard drive.
- A physical therapist uses their electronic access to look up the personal information of a friend or relative who is not currently receiving treatment from that physical therapist.

The fact that a privacy breach has occurred does not necessarily mean the practice has contravened PIPA, as certain types of privacy breaches may be unavoidable (e.g., ransomware or phishing scams carried out by sophisticated hackers). The requirement to have "reasonable" security measures does not impose a standard of perfection but requires a very high level of rigour given the sensitivity of personal information. The practice should be objectively diligent and prudent in all circumstances.

Suspected or real privacy breaches can come to a practice's attention through compliance monitoring mechanisms such as audit trails that flag unusual access, a complaint by an employee, client, or member of the public, or through the College or OIPC as a result of a formal complaint.

Anyone who reports a privacy breach in good faith and on the basis of reasonable belief is protected under PIPA's whistle-blower provisions. These provisions protect an individual from being dismissed, suspended, demoted, disciplined, harassed or otherwise disadvantaged for having reported the breach, and the individual's identity may be kept confidential by the OIPC.

The OIPC has prepared guidance materials to assist in detecting, responding to, and preventing privacy breaches. The guidance materials include:

- Privacy Breach Checklist to evaluate the impact of a privacy breach and determine if notification (see step 3 below) is necessary.
- Online Privacy Breach Report Form if an organization decides to self-report a privacy breach to the OIPC.

For more information, see *Privacy Breaches: Tools and Resources*.

Once a privacy breach is identified, the practice must respond to the breach by immediately taking four key actions.

Step 1: Contain the Breach

Take immediate steps to contain the breach and mitigate the risk of harm by:

- contacting the designated privacy officer
- immediately containing the breach, which could involve stopping the unauthorized practice, suspending user accounts, revoking computer access codes, shutting down the system that was breached, recovering the records, or correcting weaknesses in physical security
- notifying law enforcement if the breach involves theft or criminal activity
- making sure evidence that could be used to investigate or correct the breach is not compromised

Step 2: Evaluate the Risks Associated with the Breach

As soon as possible after discovering a breach, determine the extent of the breach and potential harms that could occur as a result, by considering:

- What kinds of personal information were involved and how sensitive is that information?
- What format was the information in (paper, electronic) and how was it protected (encrypted, anonymized, password protected)?
- Was it lost, stolen or mistakenly disclosed?
- Could the personal information be misused, and if so, how?
- What was the cause of the breach?
- Was it an isolated event or is there a risk of ongoing or further exposure?
- Who and how many individuals were affected by the breach?

- What harm to the affected individual(s) could result from the breach?
- Is there a relationship between the unauthorized recipients and the data subject? (A close relationship between the victim and the recipient could increase the likelihood of harm).
- What harm could result to the practice as a result of the breach?
- Are there risks to the public (such as health and/or safety) as a result of the breach?
- Has the information been recovered?

Step 3: Implement Notification Procedures

Consider whether the following individuals or groups need to be notified:

- individuals (whether clients or staff) whose personal information was involved in the breach
- the OIPC
- law enforcement authorities
- professional regulatory bodies (such as the College of Physical Therapists of BC)
- professional malpractice insurance provider
- other groups based on legal, professional, or contractual obligations

In determining whether to notify consider:

- Do any legal obligations (contractual, legislated, etc.) require notification?
- How sensitive was the personal information?
- How many people were affected by the breach?
- Was the information fully recovered without further disclosure?
- Could the personal information be used to commit fraud or identity theft?
- Is there is a reasonable risk of physical harm, psychological harm (including humiliation or damage to reputation), or financial harm (including loss of business or employment opportunities)?
- Is there is a risk of harm to the public or to client relations?

If notifying individuals who are affected by a privacy breach will avoid or mitigate harms that they could experience as a result of the breach, they should be notified immediately. While PIPA does not currently include an explicit requirement for organizations to report breaches to the OIPC, doing so will assist the practice to demonstrate that it has taken reasonable steps to respond to the privacy breach and in the resolution of any complaint should one be made to the OIPC.

The notification should include:

- the date and description of the privacy breach
- a description of the personal information that was involved in the privacy breach
- a description of potential risks of harm that could occur as a result of the breach
- steps taken to mitigate the harm
- steps planned to prevent privacy breaches in the future
- what affected individuals can do to further protect themselves and mitigate the risk of harm
- if appropriate in the circumstances, an offer for complimentary credit monitoring
- contact information for the practice's privacy officer who can answer questions
- a statement of the right to complain to the College of Physical Therapists of BC, and whether or not the practice has notified the OIPC

Step 4: Prevent Future Privacy Breaches

Once immediate steps have been taken to mitigate the risks, the practice, including the staff, should investigate the cause of the breach. Long-term safeguards should be developed to prevent further breaches. This may require updating privacy and security policies, performing a security audit of the practice's physical and technical safeguards, re-training employees on their privacy obligations, and undertaking a final audit to verify that the security arrangements have been implemented and function as planned.

Guidelines for Responding to Client and Employee Complaints

THIS SECTION WILL:

- ✓ EXPLAIN CLIENTS' AND STAFF'S RIGHTS REGARDING COMPLAINTS RELATED TO THEIR PERSONAL INFORMATION
- ✓ IDENTIFY THE REQUIREMENTS OF AN EFFECTIVE COMPLAINT MANAGEMENT PROCESS
- ✓ DESCRIBE THE STEPS OF MANAGING A COMPLAINT

Under PIPA, a practice must have a process to respond to complaints about its privacy practices or how personal information was handled. For example, individuals may have a complaint about collection practices, a disclosure of personal information without consent, a privacy breach, or the scope of records provided by the practice in response to a request for their personal information. Having an accessible and effective complaint management process is an important aspect of managing privacy risks and helps to promote accountability, openness and trust. It also allows a practice to address complaints in a timely manner, identify systemic or ongoing compliance issues and demonstrate a commitment to privacy.

In a complaint involving a privacy breach, responding in an effective and timely manner is critical. For guidance on responding to privacy breaches see *Privacy Breaches: Tools and Resources*.

Best practices for setting up a complaint management process include the following steps:

- Decide who in the practice will be responsible for receiving, responding to and managing complaints about the practice's compliance with PIPA (this could be the designated privacy officer or it could be delegated to another individual).
- Develop and document a complaint procedure that is confidential, accessible, simple and easy to use.
- Develop a complaint form to assist in recording the complaint and collecting the necessary information required to investigate and respond.
- Document the process and ensure all staff are aware of the complaint management process so they can direct a complainant to the appropriate person for follow-up or, in the absence of this individual, provide information to the complainant on how they may proceed with a complaint.
- Ensure the process includes providing reasons for a decision in sufficient detail to suit the nature of the complaint.
- Reinforce that addressing a complaint quickly helps maintain or even increase the client's trust in the practice.

Steps for Managing a Complaint

When the complaint is received in writing, record the date of the complaint and acknowledge its receipt.

- If the complaint is received verbally, record the nature of the complaint and the details.
- If necessary, contact the individual to clarify the complaint.
- Ensure that the complaint process is fair, impartial, and confidential.
- Investigate the complaint by gathering information and fully understanding the circumstances. Clarify specifics of the complaint by asking questions such as:
    - What events led to the complaint?
    - What personal information is involved and what happened to it?
    - When and where did the event(s) occur?
    - Who was involved (e.g., employees, physical therapists, student physical therapists, third party contractual employees)?
- Where a complaint is substantiated, determine the specific cause and
    - take measures to remedy the situation
    - communicate this to relevant employees involved
    - record all decisions and actions taken to prevent recurrence
- If a complaint cannot be substantiated, document the investigation so it can be explained to the complainant.
- Notify the complainant of the outcome and the reasons for the decision regardless of whether the complaint can be substantiated or not. Where applicable, inform them of the steps taken to rectify the concerns.
- Inform the complainant of the right to appeal to the OIPC, if they are not satisfied with the practice's response to the complaint, within 30 business days starting from the date the physical therapist's office communicated to the complainant its reasons for the response.
- If applicable, prevent recurrence through techniques such as modifying or updating policies and procedures, providing employee training and implementing improved privacy and security safeguards.

Guidelines for Responding to Client Requests to Access their Personal Information

THIS SECTION WILL:

- ✓ EXPLAIN CLIENTS' RIGHTS TO ACCESS THEIR PERSONAL INFORMATION HELD IN A PRACTICE
- ✓ IDENTIFY WHAT A PHYSICAL THERAPIST OR PRIVACY OFFICER SHOULD CONSIDER BEFORE RESPONDING TO ACCESS REQUESTS, INCLUDING TIMELINES, EXCEPTIONS TO DISCLOSURE OF PERSONAL INFORMATION, WHETHER TO CHARGE A MINIMAL FEE AND WHAT TO DO IF AN EMPLOYEE OR CLIENT MAKES A COMPLAINT WITH RESPECT TO ACCESS

Under PIPA, clients (or the client's legally authorized representative) and staff (including volunteers) are entitled to access their personal information in the control of a practice. Practices have a legal duty to make reasonable efforts to assist an individual with their request, respond to requests as accurately and completely as reasonably possible and, where appropriate, provide the individual with the requested personal information.

Timeline

A client must make a request to access their personal information in writing, and the practice must respond within **30 working days** of receiving a request (See form *Request for Access to Personal Information*). The response may be a copy of the clinical record or in the case where copies cannot be made, how to make arrangements for the client to review the original records.

Exceptions

There are some exceptions where personal information may not or must not be released to a client. An organization is not required to disclose personal information where:

- information is protected by solicitor-client privilege
- disclosure of the information would reveal confidential commercial information that if disclosed could, in the opinion of a reasonable person, harm the competitive position of the organization

An organization must not disclose personal information where the disclosure:

- would reveal personal information about another individual
- could reasonably be expected to threaten the safety or physical or mental health of an individual other than the individual who made the request
- can reasonably be expected to cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request
- would reveal the identity of an individual who has provided personal information about another individual and the individual providing the personal information does not consent to disclosure of their identity

PIPA allows an organization to disclose information about the mental or physical health of a client to a health care professional for the purpose of obtaining an assessment from that health care professional about whether the disclosure of information to the client could reasonably be expected to result in grave and immediate harm to the client's safety or mental or physical health. PIPA defines a "health care professional" as a medical practitioner, psychologist, registered nurse or registered psychiatric nurse. There are additional requirements for this type of disclosure, including that the practice and the health professional enter into a **confidentiality agreement** and that the information must not be used for any purposes other than making an assessment.

If the client's access request is refused, the practice must provide the client with reasons for the refusal.

Fees

The practice may charge a minimal fee for responding to a request for access to personal information. The minimal fee charged for access is intended to recover some of the actual and necessary costs incurred by the practice to provide access and it may include the costs associated with:

- locating and retrieving
- producing and copying
- preparing for disclosure
- postage or shipping costs

The fee must not generate profit, and does not usually include reviewing the records to make sure the practice is complying with its obligation in PIPA to withhold information.

When charging fees, the practice must provide the applicant with a written estimate of the total fee, and may require the applicant to pay a deposit for all or part of the amount before processing the request.

It should be noted that if a staff member makes the request, no fee can be charged for providing access to that person's employee personal information. "Employee personal information" is defined in PIPA as personal information about an individual that is collected, used, or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship.

Complaints About Access

The practice must educate staff on how to appropriately respond to such requests. If a client or staff member is not satisfied with the response, they may ask the physical therapist to reconsider the response and address the complaint internally. If the complaint cannot be resolved, the practice should inform the complainant that they may contact the College of Physical Therapists of BC to resolve the matter. The complainant should also be informed that they have 30 business days to make a formal complaint to the OIPC, starting from the date that the physical therapist communicates to the complainant its reasons for the response.

Guidelines for Secondary Use of Personal information for Research

THIS SECTION WILL:

- ✓ SUMMARIZE THE REQUIREMENTS UNDER PIPA REGARDING CLIENT CONSENT FOR THE USE OF PERSONAL INFORMATION FOR RESEARCH PURPOSES
- ✓ IDENTIFY KEY CONSIDERATIONS FOR PHYSICAL THERAPISTS WHO WISH TO DISCLOSE PERSONAL INFORMATION TO EXTERNAL HEALTH RESEARCHERS

Physical therapists must obtain consent for secondary uses, such as research, before using personal information that was initially collected for clinical purposes. While consent for the change in use from clinical to research purposes can be either written or verbal, having the client sign a consent form is best practice.

Consent is also required if a physical therapist wishes to disclose personal information to external health researchers, such as those affiliated with universities, health authorities or other health care organizations. If it is impractical to seek consent, PIPA authorizes the disclosure of personal information without consent for research purposes if all of the following conditions are met:

- The research purpose cannot be accomplished unless the personal information is provided in an individually identifiable form.
- The disclosure is on condition that it will not be used to contact persons to ask them to participate in the research.
- Linkage of the personal information to other information is not harmful to the individuals identified by the personal information and the benefits to be derived from the linkage are clearly in the public interest.
- The organization to which the personal information is to be disclosed has signed an agreement to comply with:
    - PIPA
    - the policies and procedures relating to the confidentiality of personal information of the practice that collected the personal information
    - security and confidentiality conditions
    - a requirement to remove or destroy individual identifiers at the earliest reasonable opportunity
    - prohibition of any subsequent use or disclosure of that personal information in individually identifiable form without the express authorization of the practice that disclosed the personal information
- It is impracticable for the practice to seek the consent of the individual for the disclosure.

There is an important exception to this authorization to disclose personal information for research purposes without consent. PIPA prohibits the disclosure of personal information for **market research purposes** to drug companies or other businesses without consent.

The use of personal information for research may require review and approval by a research ethics board. Where such review is required, the practice must refrain from disclosing personal information for research purposes until the researcher has obtained the requisite approvals.

Best Practices

After consent from the client is obtained, or the conditions outlined above are met, consider:

- de-identifying personal information to whatever extent is feasible and practical before disclosing to external health researchers
- retrieving and/or securely destroying records once the research is complete
- immediately ceasing collection, use or disclosure of the personal information unless otherwise permitted under PIPA when a client withdraws their consent to the collection, use, or disclosure of personal information for research purposes

If a client believes their personal information has been inappropriately collected, used, or disclosed for research purposes without consent, they may complain to the practice's privacy officer for review and investigation. If the client believes the matter cannot be resolved internally, the client has the right to bring the concern to the attention of the College of Physical Therapists of BC and/or to the OIPC.

Guidelines for Secure Destruction of Personal Information

THIS SECTION WILL:

- ✓ DESCRIBE BEST PRACTICES FOR THE SECURE DESTRUCTION OF PERSONAL INFORMATION
- ✓ IDENTIFY KEY CONSIDERATIONS AND ELEMENTS OF CONTRACTS WITH A SERVICE PROVIDER TO SUPPORT THE DESTRUCTION OF RECORDS

Under PIPA a practice is expected to securely dispose of documents that contain personal information that are no longer required for legal or business/professional purposes, in order to prevent unauthorized access, inappropriate use or identity theft. Physical therapists' obligations for record retention are set out in College *Standard of Practice: Privacy and Record Retention*. The goal is to permanently destroy personal information or irreversibly erase it so that it cannot be reconstructed, whether in paper or electronic format. This includes the original records and any duplicate copies of records that may have been created for use in the practice. A service provider may be contracted to provide the record destruction services.

Industry best practices for the secure destruction of data are constantly evolving and it is generally the responsibility of all parties who handle personal information to adequately protect that personal information.

Best Practices

Best practices for the secure destruction of personal information include:

- developing and implementing a retention and secure destruction policy
- disposing of paper records securely by cross-cut shredding (do not use single-strip, continuous shredding because it is possible to reconstruct the strips)
- incinerating paper records, if practical
- disposing of personal information stored on electronic devices (such as disks, CDs, DVDs, USB storage devices, and hard drives) securely by physically damaging the item and discarding it, or by using a wipe utility to remove the original information (note that deleting electronic information does not constitute destruction, and a wipe utility may not completely erase the information)
- ensuring machines such as photocopiers, fax machines, scanners or printers with storage capabilities are overwritten, erased, removed, or destroyed when the machines are replaced
- keeping a destruction log that includes the client's name, time period covered by the destroyed record(s), the method of destruction and person responsible for supervising the destruction (if applicable)
- conducting audits to ensure compliance by staff and service providers and that the retention and destruction policy is effective

Using a Service Provider to Destroy Records

When contracting a service provider to support the destruction of records,

Using a Service Provider to Destroy Records

When contracting a service provider to support the destruction of records,

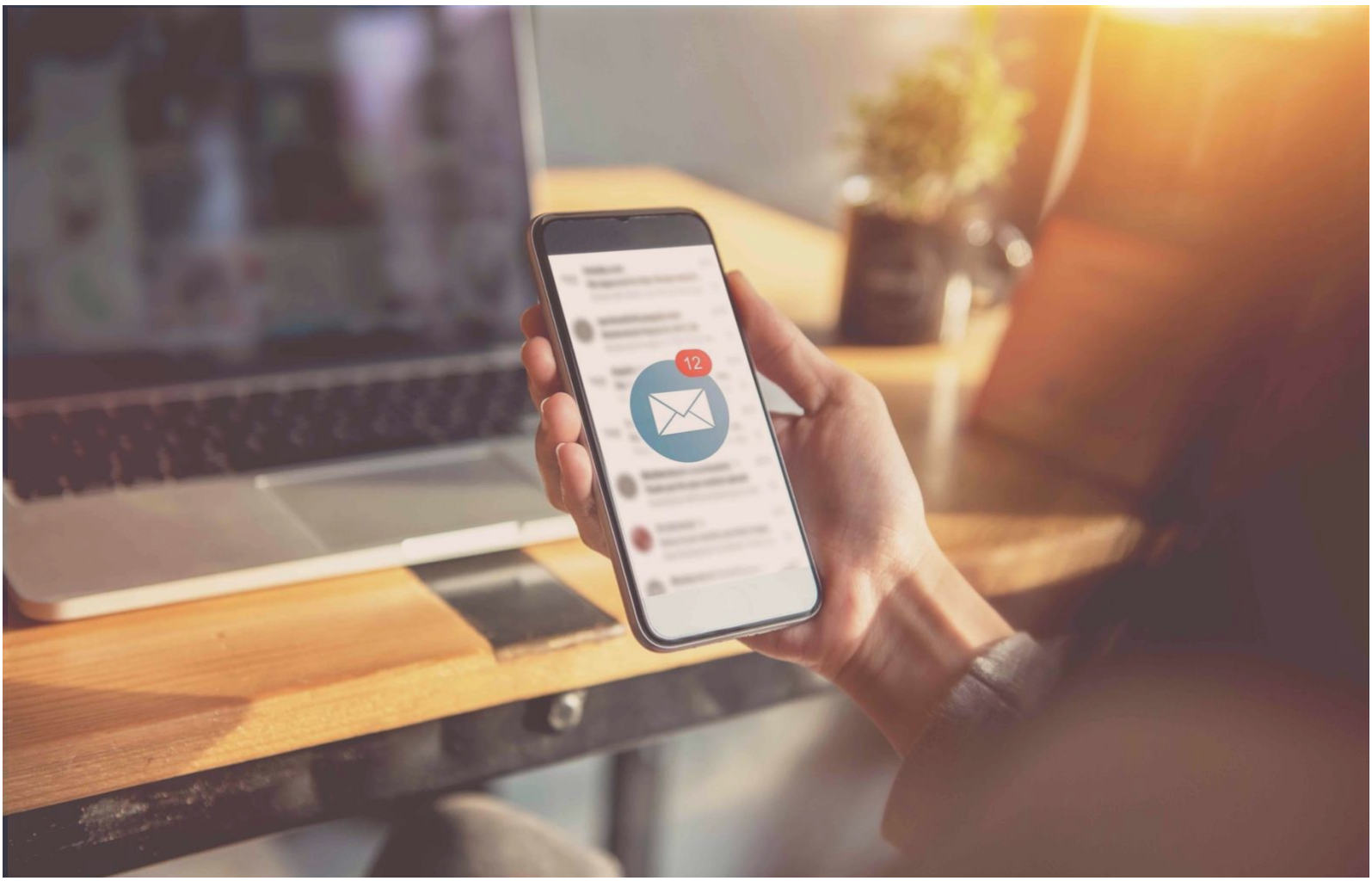
- look for one that is accredited by an industrial trade association such as the National Association for Information Destruction
- check their references
- insist on a signed contract

The contract for record destruction services usually covers these key points:

- clear description of:
    - the responsibilities of the service provider for the secure destruction of the records involved
    - how the service provider will collect the records from the practice
    - how the destruction will be accomplished for the records involved
    - what the methods are for secure storage of records pending destruction
- the limited timeframe upon which records will be destroyed
- upon request:
    - provision of a certificate of destruction documenting date, time, location, operator, and destruction method used
    - permission for an authorized person from the practice to visit the facility and/or witness the destruction
- request for proof of or requirement for staff receiving training on the importance of secure destruction of confidential personal information
- if the provider is subcontracting the destruction to a third party, require that notice be provided ahead of time with a contract in place with the third party that is consistent with the service provider's obligations to the practice

In order to have Canadian privacy protections apply to personal information, it is recommended that service providers operating within Canada be engaged. However, for a variety of reasons many service providers operate some or all portions of their services outside the country. Be sure to understand where personal information is being stored, who has access to it, what security provisions are in place, and from what locations personal information may be accessed (e.g., if there is remote access for support).

Guidelines for Use of Email or Fax



THIS SECTION WILL:

- ✓ SUMMARIZE THE BENEFITS AND PRIVACY RISKS ASSOCIATED WITH THE USE OF EMAIL OR FAX IN THE CLINICAL CONTEXT
- ✓ IDENTIFY KEY CONSIDERATIONS FOR PHYSICAL THERAPIST'S OFFICES THAT USE EMAIL OR FAX TO TRANSMIT PERSONAL INFORMATION

Physical therapists must take steps to reduce the risks associated with email or fax communications and ensure that reasonable safeguards are in place to protect personal information.

What Are the Risks?

When using email or fax to transmit personal information to clients, the following issues may negatively impact client care:

- difficulties:
  - confirming the identity of the client in an incoming email or fax
  - ensuring the correct recipient with only the client's name, email address or fax number, as clients may have similar names
- risk to clients:
  - suffering adverse health consequences if it is an urgent matter and there is a delay in the response time
  - misinterpreting the content of an email or fax, which could lead to:
    - adverse health consequences
    - a complaint
    - legal action if the client's perception is one of inadequate or ineffective communication

Using email to communicate with clients or third party health providers can give rise to the following privacy and security issues.

- An email message that is not encrypted can be:
  - intercepted by unauthorized third parties
  - altered and forwarded to unintended recipients

- Email messages containing personal information can be intercepted by unauthorized third parties if the email is:
    - delivered to the wrong address
    - sent or received from unsecured locations such as those publicly accessible or a shared home computer
    - retained on a home computer
    - sent or received using a public Wi-Fi network
    - shared by internet service providers with other third parties
    - saved on unsecured backup servers and subject to improper organizational retention rules
- Attachments in an email may contain viruses that could cause serious damage to computer systems.
- The personal information being emailed may leave Canada during transmission, and may be subject to laws in other jurisdictions that have inadequate protections or no protections at all.
- Faxing personal information can have privacy and security risks of personal information being accessed by unauthorized third parties if the fax is:
    - sent to an incorrect fax number (caused by misdialing or by pressing the wrong speed-dial key)
    - exposed to unauthorized individuals simply because the fax machine is located in an open, unsecured location
    - accessed by third parties who are tapping into or monitoring the transmission

Best Practices

Consider informing clients:

- about how emailing or faxing personal information can result in accidental disclosure or interception by other people not intended to receive the information
- what precautions the practice has taken to reduce the risks
- if the personal information is very sensitive, what other delivery options exists that are more secure (e.g., photocopies sent by mail or courier)
- that they can withdraw consent at any time to using fax or email as a method of communication, and how to do so

Office policies on use of email and fax usually include:

- criteria for the client-provider communication, acceptable use, email etiquette, and management of email documentation as part of the client's medical record

- staff training on the
    - appropriate use of email and fax
    - maintenance of emailed or faxed documents
- a process to remove a client from email or fax communications if the client withdraws consent to using any of these methods of communication
- appropriate destruction methods for emails and faxes, including deletion of emails from computer hard drive and faxes from memory

When communicating with clients or third party health care providers by email:

- Only use email systems that encrypt the email transmission and incoming and outgoing emails (or that apply other similar industry-standard protections).
- Protect each email inbox that is used to send or receive messages with a secure password known only by the individuals authorized to access the inbox.
- Protect any attached documents with a strong password and advise the recipient to let them know.
- Confirm the correct email address for the intended recipient.
- Verify email addresses regularly as they can be duplicated, and may frequently change.
- Whenever possible, leave sensitive personal information out of the email or use obscure identifiers to protect it during transmission
- Add a confidentiality disclaimer to email messages that states
    - the content is confidential and only intended for the stated recipient
    - anyone receiving the email in error must notify the sender and return or destroy the email
- For sensitive personal information, contact the recipient by phone to inform them that confidential information is being sent and ask the recipient to call back to confirm receipt.
- Never use email distribution lists to send personal information.

When communicating with clients or third party health care providers by fax:

- Only use fax systems that encrypt the fax transmission and incoming and outgoing faxes (or that apply other similar industry-standard protections).
- Protect the fax machine or the fax modem (a fax device that uses a computer program) with a secure password known only by individuals in the office who are authorized to send or receive faxes.
- Ensure the fax machine is located in a secure area in the practice to prevent unauthorized persons from viewing or receiving the documents.

- Always use a fax cover sheet that identifies both the sender and recipient with contact information and states the total number of pages being sent.
- Whenever possible, leave sensitive personal information out of the fax or use obscure identifiers to protect it during transmission
- Include a disclaimer stating
    - the faxed material is confidential and only intended for the stated recipient
    - anyone receiving the fax in error must immediately notify the sender and return or destroy the fax
- Before faxing the information, confirm the recipient's fax number (including when using a pre-programmed number)
- If using pre-programmed fax numbers, regularly verify these numbers for accuracy
- Check the fax confirmation report as soon as the fax has been sent to confirm that the fax went to the correct place and that all pages were transmitted and received
- Check each day's fax history report for errors or unauthorized faxing
- When receiving faxes
    - retrieve documents sent by fax as soon as they have been processed
    - do not leave the documents sitting on or near the fax machine
    - if a fax is received in error, promptly notify the sender and return or destroy the information

Sharing fax machines with other offices is discouraged, particularly where personal information is frequently sent and received.

Retention of Emails or Fax Documents

For storage and retention of emails and faxes, consider the following:

- Do not make or retain more copies of email communications than needed.
- Securely destroy extra copies that are no longer needed.
- Include personal information that is emailed as part of the client's clinical record.

Guidelines for Use of Mobile Devices

THIS SECTION WILL:

- ✓ SUMMARIZE THE RISKS AND BENEFITS OF USING MOBILE DEVICES TO PROVIDE HEALTH CARE SERVICES
- ✓ IDENTIFY KEY REQUIREMENTS AND BEST PRACTICES FOR USING MOBILE DEVICES

Mobile devices such as smartphones and tablets allow a physical therapist convenient and timely access to clients and other health care providers remotely. However, the use of mobile devices in a practice can create privacy and security risks to personal information. Those risks include loss or theft of the device, malicious programs that track or spy on the device and having personal information be intercepted or monitored by unauthorized third parties. Any wireless device, including a mobile device, that is connected to a network (e.g., Wi-Fi, Bluetooth, 3G and near-field communication) can serve as an illicit entry point to the entire network if it is not properly set up with appropriate security controls.

For more information on mobile devices and privacy, see: *Top 15 Tips: Mobile Devices: Tips for Security and Privacy.*

Best Practices

Physical therapists have an obligation to ensure adequate administrative, physical and technical safeguards are in place before using mobile devices in their practice. This obligation extends to staff and third parties who have access to personal information under the practice's custody or control. Physical therapists must also take reasonable steps to ensure any devices, apps or programs used by their practice comply with PIPA.

- Ensure:
  - devices have strong, up-to-date, industry-standard encryption for transmitting personal information to minimize the risk of unauthorized interception
  - devices are protected with a secure password
  - anti-malware software is installed and up to date to protect against attacks
  - any systems to which the device is connected provides adequate end-to-end security
  - any cloud services used to transmit or store data are secure and use encryption (do not use public services that can be easily accessed by unauthorized third parties)
  - voice command features are disabled if they are not needed, as this feature allows the device to always be listening
  - the screen is set to lock automatically after a short period of inactivity

- Avoid:
    - use of public Wi-Fi connections as they are vulnerable to unauthorized interception
    - modifying the operating system by jailbreaking or rooting the device as this weakens its security
- Limit:
    - the number of incorrect password attempts before the data is deleted
    - access permissions for apps, unless the permissions are related to the service
    - location information used by programs to avoid creating a log of the user's movements, which may include visits to clients' homes
- Always:
    - use apps that come from official app stores and that use strong, up-to-date, industry-standard encryption
    - keep software up to date
- Promptly report a lost or stolen device, and consider using programs that help to locate a lost phone.
- When returning or disposing of a device, ensure it is completely wiped and safely disposed of.
- Delete personal information from the device once it's been added to the client's clinical record.

It is recommended that policies regarding the use of mobile devices in a practice be included in the practice's privacy management program.

Privacy Resources for Physical Therapists

BC Privacy Legislation	
Freedom of Information and Protection of Privacy Act	http://www.qp.gov.bc.ca/statreg/stat/F/96165_01.htm
Guide to the *Personal Information Protection Act*	https://www.oipc.bc.ca/guidance-documents/1438
Personal Information Protection Act	http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01
Privacy: What Physical Therapists Need to Know	https://cptbc.org/physical-therapists/practice-resources/advice-to-consider/privacy-what-physical-therapists-need-to-know/
Codes of Ethics and Privacy	
CPTBC Code of Ethical Conduct	https://cptbc.org/legislation-standards/code-of-ethical-conduct/
CPTBC Standard 13 – Privacy/Confidentiality	CPTBC Standard of Practice: Privacy and Record Retention
Accountability	
CPTBC Bylaws- Registrant Records	https://cptbc.org//wp-content/uploads/2019/05/CPTBC-Bylaws-May-23-2019.pdf
CPTBC Standard 8 – Documentation and Record-Keeping	CPTBC Standard of Practice: Documentation
Data Handling	
Privacy Breaches: Tools and Resources	https://www.oipc.bc.ca/guidance-documents/1428
Protecting Personal Information	http://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information
Protecting Personal Information Away from the Office	https://www.oipc.bc.ca/guidance-documents/1447
Securing Personal Information: A Self-Assessment Tool for Organizations	https://www.oipc.bc.ca/guidance-documents/1439

Information Technology	
CPTBC Advice to Consider – Tele-Rehabilitation	*https://cptbc.org/physical-therapists/practice-resources/advice-to-consider/tele-rehabilitation/*
Cloud Computing for Small- and Medium-Sized Enterprises	*https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/cloud-computing/gd_cc_201206/*
Contemplating a Bring your Own Device (BYOD) Program? Consider These Tips	*https://www.oipc.bc.ca/guidance-documents/1828*
Privacy and Cybersecurity	*https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/cs_201412/*
Top 15 Tips: Mobile Devices: Tips for Security and Privacy	*https://www.oipc.bc.ca/guidance-documents/1994*
Privacy Commissioners	
British Columbia	*https://www.oipc.bc.ca*
Canada	*https://www.priv.gc.ca*

Definitions

Access

The ability to view or collect data, particularly from an electronic database. When a record is accessed, it is usually considered a disclosure by the practice. Only authorized users should be able to access personal information in an electronic record.

Application Service Provider (ASP)

A third party service provider that manages and stores the electronic record at its data centre, rather than the physical therapist managing and running servers in their own practice. Physical therapists or their authorized employees have access to the electronic record over the Internet or preferably over a private network.

Authentication

A method designed to allow a computer application to verify credentials—usually in the form of a user name and password for single-factor authentication or user name and password plus an access token for multi-factor authentication.

Collection

The act of gathering, receiving, accessing or obtaining personal information.

Confidentiality

In the health care context, it refers to a physical therapist's or other health professionals' ethical and legal obligations to protect an individual's personal information, unless the individual consents to the disclosure or the disclosure is otherwise authorized.

Consent

The authority that an organization usually needs under PIPA to collect, use or disclose an individual's personal information. Consent occurs when an individual provides verbal or written agreement to the collection, use or disclosure of their personal information, after being informed about the type of personal information being consented to, and the purposes for which the information is being collected, used or disclosed. In limited circumstances, PIPA authorizes the collection, use and disclosure of personal information without consent. Consent must be voluntary, and the physical therapist must be able to show that a reasonable person would consider the purpose for which the information is collected, used or disclosed to be appropriate in the circumstances. When providing health care services to a client, a physical therapist cannot require the client to consent to the collection, use or disclosure of personal information beyond what is necessary to provide those services. An individual has the right to withdraw or change their consent by giving reasonable notice, and the physical therapist must explain the consequences on the provision of care. See also 'Implicit Consent'.

Data Masking

The process of restricting access to data in an electronic record by substituting real values with random characters that obfuscate or disguise the data. Data Masking can be applied at different levels of granularity depending on the unique circumstances and system capabilities.

Data Stewardship

Also known as accountability, the legal, ethical and fiduciary responsibilities of a physical therapist in managing and protecting personal information including collection, use, disclosure and retention.

Disclosure

Sharing, exposing or providing access to information, including to another organization, third party or to the individual the information is about.

Electronic Record

An electronic record system within a practice that enables a health care professional, such as a physical therapist, to record and store the information collected during a client's visit instead of, or in addition to, a paper file. The electronic record may also allow the physical therapist to access personal information from other electronic health record systems.

Electronic Record Service Provider

A third party service provider that sells and supports electronic record software.

Encryption

The process of protecting personal information by encoding data into an electronic form that can only be read by the intended authorized recipient. All personal information of a sensitive nature should generally be encrypted.

Freedom of Information and Protection of Privacy Act (FIPPA)

BC privacy legislation that governs how personal information is collected, used, disclosed and protected by public bodies, including health authorities and the Ministry of Health.

Health Authority

Includes the following entities that deliver health care services to British Columbians:

- Provincial Health Services Authority
- five regional health authorities:
    - Fraser Health
    - Interior Health
    - Northern Health
    - Vancouver Coastal Health
    - Vancouver Island Health
- First Nations Health Authority
- Providence Health Care

All personal information collected, used and disclosed by the health authorities is governed by FIPPA with the exception of the First Nations Health Authority which is governed by PIPA. This Toolkit uses the term to refer to the health authorities that are governed by FIPPA.

Implicit Consent

An individual's implicit agreement to the collection, use or disclosure of their personal information by an organization. Implicit consent (see Section 8(3) of PIPA) is a form of implied consent that occurs when an individual receives notice, in a manner the individual can reasonably be expected to understand, that their personal information will be collected, used or disclosed for a specific purpose. The individual must also be provided with a reasonable amount of time to decline after being informed. The collection, use or disclosure must be reasonable, given the sensitivity of the information in the circumstances, and must be limited to the purpose set out in the notice.

Mobile Device

A handheld mobile device that provides computing, information storage or retrieval capabilities for personal or business use (e.g., smartphone). Such devices are frequently used to maintain an electronic schedule or contact information, and in some cases store clients' personal information.

"Need to Know" and "Least Privilege" Principles

The "need to know" principle states that authorized users of a system should only have access to the minimum amount of personal information that is necessary to perform their duties within a public body or an organization. The "least privilege" principle requires that each authorized user in a system be granted the most restrictive access privileges needed for performing authorized tasks. The principles are reflected in privacy law but not always expressly stated.

Personal Information

Information, including personal health information, about an identifiable individual which includes factual or subjective information about that individual. This information includes, but is not limited to, name, personal address, birth date, physical description, medical history, gender, education, employment and visual images such as photographs or videotapes.

Personal Information Protection Act (PIPA)

BC privacy legislation that governs how personal information is collected, used, or disclosed, and protected by private sector organizations, including physical therapists' private practices and other private health care facilities.

Personal Information Protection and Electronic Documents Act (PIPEDA)

Federal legislation that governs the collection, use and disclosure of personal information by federally regulated private sector organizations.

Privacy

The right to be free from intrusion, influence or interruption and to control one's personal information. It is linked with other fundamental rights such as freedom of expression, security of the person, dignity and personal autonomy. Privacy also includes the right of individuals to determine when, how and to what extent they share information about themselves with others.

Privacy Breach

Unauthorized access, collection, use, disclosure, or disposal of personal information.

Privacy Management Program

A program that demonstrates an organization's accountability for personal information and capacity to comply with applicable privacy laws and related industry standards, as well as correctly identifying, addressing or minimizing privacy-related obligations and risks. Includes appointing a privacy officer, responding to requests for access and complaints under PIPA, and developing, implementing, maintaining and updating policies, systems, procedures and training for collection, use, disclosure, consent, notification, access to information, retention, disposal, privacy breaches and corrections.

Privacy officer

The individual designated to be accountable for ensuring organizational compliance with privacy legislation, industry standards for privacy and privacy-related professional and regulatory obligations. The responsible physical therapist may choose to delegate responsibilities for the privacy management program to an employee but they remain ultimately responsible.

The privacy officer is responsible for

- developing policies and procedures
- implementing program controls
- designing and implementing employee training and education
- conducting ongoing assessments and revising program controls
- monitoring for compliance
- managing privacy breach incidents
- managing complaints
- answering questions
- responding to requests for access to or correction of personal information
- demonstrating leadership in creating and maintaining a culture of privacy
- being informed of any privacy related changes in legislation

Private Network

A secure, private, end-to-end network that allows secure, high-speed access to an electronic record, secure Internet access and secure email messaging.

Reasonable Security Measures

The measures taken to protect personal information from unauthorized collection, use or disclosure by implementing physical controls (e.g., locked cabinets, securely stored laptops or key card access), technical controls (e.g., firewall, document encryption or user access profiles) and administrative controls (staff training, privacy policy or retention and destruction policy). Factors to consider when implementing reasonable measures include the sensitivity of the personal information (clinical records are considered highly sensitive), the likelihood of a privacy breach, the harm caused if a breach occurred, the type of record involved, the cost of the security measures and current industry standards.

Remote Access

The ability to get secure access to a computer or network from outside the practice. Individuals who are travelling or working from home may need access to information and may access the network and systems remotely.

Role-Based Access

A policy and technical architecture involving the assignment of access privileges to roles based on job functions rather than to individual users. Users are granted privileges in accordance with the “need to know” and “least privilege” principles by virtue of being authorized to act in specific roles.

Security

Controls that protect personal information from unauthorized collection, use or disclosure. Examples include locking cabinets, or in relation to electronic records, password protections, encryption and firewalls.

Staff

May include employees, locum physical therapists, associates, students, student physical therapists, contractors and volunteers with whom you collect, use or disclose personal information.

Strong Password

A password that is sufficiently long or random such that it is producible only by the user who creates it. It is case sensitive and includes a random combination of alphanumerics and symbols. The College recommends that a strong password should be eight or more characters in length and contain at one or more numbers, upper and lower case letters and symbols (e.g., IloveParis!936).

Third Party

In the context of personal information that is controlled by a practice, refers to anyone outside the practice or the individual the information is about.

Two Factor Authentication

The combination of user name/password (something an authorized user knows) and some other physical identification tool like a secure ID token (something an authorized user has), which are both required in order to verify the identity of a person.

Use

Any operation (other than collection or disclosure) performed on, or use made of, personal information by the practice or third party that collected the information for a specified purpose.

Virtual Private Network (VPN)

An authentication and encryption method that allows connection from outside the practice to the electronic record over the Internet with enhanced security.