Active Care Physiotherapy Privacy Policy

Privacy of personal information is an important principle to Active Care Physiotherapy. We are committed to collecting, using and disclosing personal information responsibly and only to the extent necessary for the goods and services we provide. We also try to be open and transparent as to how we handle personal information. This document describes our privacy policies.

What is Personal Information?

Personal information is information about an identifiable individual. Personal information includes information that relates to their personal characteristics (e.g., gender, age, income, home address or phone number, ethnic background, family status), their health (e.g., health history, health conditions, health services received by them) or their activities and views (e.g., religion, politics, opinions expressed by an individual, an opinion or evaluation of an individual). Personal information is to be contrasted with business information (e.g., an individual's business address and telephone number), which is not protected by privacy legislation.

Who we are

Our organization, Active Care Physiotherapy Inc.*,* includes at the time of writing three Physiotherapists, one Massage Therapist and two support staff. We use a number of consultants and agencies that may, in the course of their duties, have limited access to personal information we hold. These include computer consultants, office security and maintenance, bookkeepers and accountants, temporary workers to cover holidays, credit card companies, website managers, cleaners and lawyers. We restrict their access to any personal information we hold as much as is reasonably possible. We also have their assurance that they follow appropriate privacy principles.

We collect personal information: primary purposes

About Clients

Like all healthcare providers, we collect, use and disclose personal information in order to serve our clients. For our clients, the primary purpose for collecting personal information is to provide treatment. For example, we collect information about a client's health history, including their family history, physical condition and function and social situation in order to help us assess what their health needs are, to advise them of their options and then to provide the health care they choose to have. A second primary purpose is to obtain a baseline of health and social information so that in providing ongoing health services we can identify changes that are occurring over time. It would be rare for us to collect such information without the client's express consent, but this might occur in an emergency (e.g., the client is unconscious) or where we believe the client would consent if asked and it is impractical to obtain consent (e.g., a family member passing a message on from our client and we have no reason to believe that the message is not genuine).

We collect personal information: secondary purposes

Like most organizations, we also collect, use and disclose information for purposes related to or secondary to our primary purposes. The most common examples of our related and secondary purposes are as follows:

1. To invoice clients for goods or services that were not paid for at the time, to process credit card payments or to collect unpaid accounts.
2. To advise clients that their product or service should be reviewed (e.g., to ensure a product is still functioning properly and appropriate for their then current needs and to consider modifications or replacement).
3. To advise clients and others of special events or opportunities (e.g., a seminar, development of a new service, arrival of a new product) that we have available.
4. Our clinic reviews client and other files for the purpose of ensuring that we provide high quality services, including assessing the performance of our staff. In addition, external consultants (e.g., auditors, lawyers, practice consultants, voluntary accreditation programs) may on our behalf do audits and continuing quality improvement reviews of our Clinic, including reviewing client files and interviewing our staff.
5. Physiotherapists are regulated by the College of Physiotherapists of Ontario who may inspect our records and interview our staff as a part of their regulatory activities in the public interest. In addition, as professionals, we will report serious misconduct, incompetence or incapacity of other practitioners, whether they belong to other organizations or our own. Also, our organization believes that it should report information suggesting serious illegal behaviour to the authorities. External regulators have their own strict privacy obligations. Sometimes these reports include personal information about our clients, or other individuals, to support the concern (e.g., improper services). Also, like all organizations, various government agencies (e.g., Canada Customs and Revenue Agency, Information and Privacy Commissioner, Human Rights Commission, etc.) have the authority to review our files and interview our staff as a part of their mandates. In these circumstances, we may consult with professionals (e.g., lawyers, accountants) who will investigate the matter and report back to us.
6. The cost of some goods/services provided by the organization to clients is paid for by third parties (e.g., OHIP, WSIB, private insurance, Assistive Devices Program). These third-party payers often have your consent or legislative authority to direct us to collect and disclose to them certain information in order to demonstrate client entitlement to this funding.
7. Clients or other individuals we deal with may have questions about our goods or services after they have been received. We also provide ongoing services for many of our clients over a period of months or years for which our previous records are helpful. We retain our client information for a minimum of ten years after the last contact to enable us to respond to those questions and provide these services (our regulatory College also requires us to retain our client records).
8. If Active Care Physiotherapy or its assets were to be sold, the purchaser would want to conduct a “due diligence” review of the Clinic’s records to ensure that it is a viable business that has been honestly portrayed to the purchaser. This due diligence may involve some review of our accounting and service files. The purchaser would not be able to remove or record personal information. Before being provided access to the files, the purchaser must provide a written promise to keep all personal information confidential. Only reputable purchasers who have already agreed to buy the organization’s business or its assets would be provided access to personal information, and only for the purpose of completing their due diligence search prior to closing the purchase.

You can choose not to be part of some of these related or secondary purposes (e.g., by declining to receive notice of special events or opportunities, by paying for your services in advance). We do not, however, have much choice about some of these related or secondary purposes (e.g., external regulation).

About Members of the General Public

For members of the general public, our primary purposes for collecting personal information are to provide notice of special events (e.g., a seminar or conference) or to make them aware of services in general or our clinic in particular. For example, while we try to use work contact information where possible, we might collect home addresses, fax numbers and email addresses. We try to obtain consent before using any such personal information, but where this is not, for any reason, possible, we will upon request immediately remove any personal information from our distribution list.

On our website we only collect, with the exception of cookies, the personal information you provide and only use that information for the purpose you gave it to us (e.g., to respond to your email message, to register for a course, to subscribe to our newsletter). Cookies are only used to help you navigate our website and are not used to monitor you.

About Contract Staff, Volunteers and Students

For people who are contracted to do work for us (e.g., temporary workers), our primary purpose for collecting personal information is to ensure we can contact them in the future (e.g., for new assignments) and for necessary work-related communication (e.g., sending out paycheques, year-end tax receipts). Examples of the type of personal information we collect for those purposes include home addresses and telephone numbers. It is rare for us to collect such information without prior consent, but it might happen in the case of a health emergency (e.g., a SARS outbreak) or to investigate a possible breach of law (e.g., if a theft were to occur in the clinic). If contract staff, volunteers or students wish a letter of reference or an evaluation, we will collect information about their work related performance and provide a report as authorized by them.

Protecting Personal Information

We understand the importance of protecting personal information. For that reason, we have taken the following steps*:*

1. Paper information is either under supervision or secured in a locked or restricted area.
2. Electronic hardware is either under supervision or secured in a locked or restricted area at all times. In addition, passwords are used on computers. All of our cell phones are digital, as such signals are more difficult to intercept.
3. Paper information is transmitted through sealed, addressed envelopes or boxes by reputable companies.
4. Electronic information is transmitted either through a direct line or is anonymized or encrypted.
5. Staff is trained to collect, use and disclose personal information only as necessary to fulfill their duties and in accordance with our privacy policy. Training is provided to staff on who collects what personal information; consent forms required, and restricting collection of personal health information to the purposes identified in Privacy Statement. Privacy Training occurs for each new hire and will be reviewed with all staff members annually.

6. Authorized individuals who have remote access to PHI have appropriate security systems in place and have signed the appropriate Confidentiality Agreement. They ensure at all times that PHI is being protected from unauthorized individuals
7. External consultants and agencies with access to personal information must enter into privacy agreements with us.
8. Service providers, employees, external staff, volunteers or any other external agency that comes into contact with PHI must read and sign our confidentiality agreement. A copy of each confidentiality agreement is held with the Privacy Officer.

Consent

Consent must be obtained to collect, use or disclose personal health information. To be capable of consenting, a patient must be able to understand:

1. The information needed to make a decision on whether or not the patient should consent to the collection, use or disclosure of personal health information, and
2. The consequences of giving, withholding or withdrawing consent.
3. When a patient is not capable of providing consent you may get consent from a Substitute Decision Maker (SDM) (ranked in order as listed) from the patient's:
    a. Guardian (if guardian has the authority to make such decisions)
    b. Attorney for personal care or attorney for property (if the attorney has authority)
    c. Representative (appointed by Capacity Board)
    d. Spouse or partner
    e. Child, custodial parent, or children's aid society or other person legally entitled to give or withhold consent in place of a parent)
    f. Parent with access rights
    g. Brother or sister, and
    h. Any other relative (related by blood, marriage or adoption).
    i. If the patient has died, you can get consent from the patient's estate trustee or someone in charge of administering the patient's estate.
    j. To consent for a patient, the person must be:

- included in the list above,
- available and capable of consenting,
- at least 16 years old or the patient's parent,
- willing to assume responsibility for giving or refusing consent,
- free of any court order or separation agreement prohibiting them from having access to or consenting for the patient,

and the highest ranked person on the list of potential substitute decision-makers who is available and capable of consenting.

Patients may withdraw their consent at any time.

i. Patients who want to withdraw their consent must notify us that they no longer consent to our collection, use and disclosure of their personal health information using the Withdrawal of Consent Form/Consent Directive Form
ii. Patient/ Substitute Decision Makers (SDM) have the right to impose a Consent Directive on the access/use of their Personal Health Information (PHI) in whole or in part.
iii. Patient/ Substitute Decision Makers (SDM) wishing to impose their right to a Consent Directive must sign the Withdrawal of Consent Form. This form is then forwarded to the Privacy Officer who will incorporate it into the patients Electronic Medical Record (EMR).
iv. A patient's withdrawal has no effect on information collected, used or disclosed before the patient withdrew consent, but has effect from the time it is received.
v. If the withdrawal of consent will compromise patient care, the effect of the withdrawal will be discussed and documented in the patient's health record.
vi. When Active Care Physiotherapy discloses personal health information to others, it is required to tell them when it thinks that information is inaccurate or incomplete, including when it thinks the missing information could affect patient health care.

Disclosure Tables

The issue of disclosure is complex. Table A1 – A4 in the appendix provides a pictorial representation of the most common examples of disclosures to help you determine when disclosure must or can be made.

Mandatory Disclosure

The Act specifically permits the disclosure of personal health information for a number of purposes as required by other statutes. Consent is not required for these specific purposes. See Table A1 to A4 in the appendix for more information.

Health Information Custodian (HIC) and Personal Health Information (PHI)

A HIC may disclose PHI (that is subject to a consent directive) to another HIC if the other HIC:

1) Obtains the express consent of the individual to whom the information relates;

2) Believes on reasonable grounds, that the collection is necessary for the purposes of eliminating or reducing a significant risk of serious bodily harm to the individual to whom the information relates and it is not reasonable for the other HIC to obtain consent in a timely manner;

3) Believes on reasonable grounds, that the collection is necessary for the purposes of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom the information relates or to a group of persons. When this occurs, Active Care Physiotherapy would be required to immediately provide written notice (in accordance with the regulations) to the HIC who collected the information (the HIC who effected the consent override), and the HIC would be required (at the first reasonable opportunity) to notify the individual to whom the information relates.

A Privacy Breach

A privacy breach occurs when there is unauthorized access to or collection, use or disclosure of personal information. There are 3 levels of privacy breach and consequences.

1. **Maximum Breach**

Examples include but are not limited to:

a) Theft or Loss of equipment that is perceived to contain PHI
b) Unauthorized access to or collection, use or disclosure of PHI for malicious intent
c) Deliberate disregard for Privacy Agreement

This action could result in:
- Termination of employment/contract and/or possible legal action Investigation brought forward to the employee's college of profession (CPSO, CNO)
- Information Privacy Commissioners of Ontario's Involvement
- Client being notified of incident

2. **Medium Breach**

Examples include but are not limited to:

a) Sensitive information being stored on unsecure portable devises (laptop, blackberry, memory stick etc.)
b) Release of PHI to the incorrect health care provider
c) Disclosure of PHI to a third party without express consent
d) Viewing of Family, Friends, Neighbour PHI in our data base or in any other Health Service Provider database that has been granted authorized access
e) Releasing PHI via non-secure or not approved mediums as outlined in Privacy Statement; leaving PHI in visible view' in car' on desk in common work areas etc.

f) Failure to comply with 3 verbal warnings

This action could result in:
- Being brought before the Privacy Officer and Organization Executive.
- Record of infraction being documented in personnel file.
- Investigation brought forward to the employee's college of profession (CPSO, CNO)
- Information Privacy Commissioners of Ontario's Involvement
- Client being notified of Incident

3. Minimum Breach

Examples include but are not limited to:

a) Leaving PHI in plain view on computer when not at your desk
b) Allowing others to use your password
c) Not taking reasonable measures to avoid accidental exposure to PHI like 'reader over the shoulder' or discussing PHI at a loud volume in an area where it may be overheard by inappropriate individuals.
d) Not taking reasonable means to ensure PHI is released to appropriate individuals
e) Not signing out computer equipment

This action could result in:
- Written and/or oral warning that may be documented in Personnel file.

Safeguarding Personal Health Information: Staff Training

We provide training on who collects what personal information; consent forms required, and restricting collection of personal health information to the purposes identified in Privacy Statement. Privacy Training will occur for each new hire and will be reviewed with all staff members annually.

Here is a simple list of staff dos and don'ts as it pertains to personal health information at Active Care Physiotherapy.

Do:

- Use only approved devices or processes to access PHI
- Use only your own login & protect it – no sharing - you are accountable for any actions tracked to your login account
- Use encrypted devices and only store the minimum amount of PHI necessary on a portable device
- Change your password if you feel it may have been compromised and notify your Privacy Officer
- Create strong and "hard-to-guess" passwords & keep your password a secret!
- Never create a password that includes your ID, 3 consecutive letters, an easily recognized patterns or easily obtained personal information about yourself (e.g., pet's name)
- Create a unique password (i.e., different from your email or bank account)

- Commit your password to memory – only record it if it can be stored securely
- Use phrases when creating your password (e.g., ILOv2EatPizza)

Don't:
- Disable, bypass or override any information security controls (e.g., virus protection)
- Leave a computing device in public places or in your car in plain view – take it with you or lock it in your trunk
- Share PHI with anyone except as authorized and required for your job
- Discuss or access PHI in public places where others may see the information
- Leave your login open & unattended i.e., log off or lock your computer device
- Take a picture of PHI displayed on a device
- Attempt to exploit a real or suspected security weakness
- Do something that you know will interfere with the system's normal operations or the integrity of the data processed by the system
- Email PHI outside your organization's secure email system unless it is encrypted

The privacy officer will ensure that technological security (ie: passwords, encryption, firewalls and software) are up to date and ensure that wireless data has appropriate level of security. Network is not broadcasted and access is controlled.

Individual access

Except under special circumstances, patients have the right to access their personal health records. Patients or their Substitute Decision Makers may request access to their personal health records in writing by completing the Patient Request to Access Form. In some circumstances a verbal request is acceptable.

When a request has been received we:

1. Verify the patient's identity.
2. Locate record and verify it is the correct PHI for the request by confirming name, date of birth, or health card number. If record cannot be located contact the requestor in writing asking for more information.
3. Collection and release of PHI will be completed within 30 days of receipt of written request.
4. Written notice of extension should explain when you will respond and why the extension is needed. An extension cannot exceed an additional 30 days.
5. Determine if one of the legal exceptions applies to providing access.

Accuracy

When making a correction we record and date the correct information in the record and cross out the incorrect information (without obliterating it). If that is not possible, we date and label the information as incorrect. The Clinician/staff member who initially charted the record in question will validate the request and correct the personal health record within 30 days.

Retention and destruction of personal information

We need to retain personal information for some time to ensure that we can answer any questions you might have about the services provided and for our own accountability to external regulatory bodies. However, we do not want to keep personal information too long in order to protect your privacy.

We keep our adult client files for ten years from the last entry date. We keep our minor client files for 10 years after the patient would have turned 18. If a notice for an investigation or inspection under the *Regulated Health Professions Act*, *Health Insurance Act* or *Coroners Act* is received, the records must be retained until the investigation or inspection and any subsequent hearing is completed.

Where a claim of negligence may arise: adult files must be kept a minimum of 15 years from the date on which the act or omission upon which the claim of negligence could be based occurred. Minors files must be kept a minimum period of 15 years from the date the patient turned 18. In both cases, if the patient cannot commence a claim because of a mental, physical or psychological condition and the individual has no litigation guardian, the records should be kept longer.
The rules around discoverability of a negligence claim are complex and are dependent on the specific facts of each case.

Our client and contact directories are much more difficult to systematically destroy, so we remove such information when we can if it does not appear that we will be contacting you again. However, if you ask, we will remove such contact information right away. We keep any personal information relating to our general correspondence (e.g., with people who are not clients) newsletters, seminars and marketing activities for about six months after the newsletter ceases publication or a seminar or marketing activity is over.

We destroy paper files containing personal information by shredding. We destroy electronic information by deleting it and, when the hardware is discarded, we ensure that the hard drive is physically destroyed. Alternatively, we may send some or the entire client file to our client.

A log will be filled out stating the names of the patients whose records where disposed of, the dates the records were disposed of and the disposal procedure. This electronic log will be kept by the Privacy Officer Indefinitely.

You can look at your information

You have the right to see what personal information we hold about you. All you have to do is ask. We can help you identify what records we might have about you. We will also try to help you understand any information you do not understand (e.g., short forms, technical language, etc.). We will need to confirm your identity, if we do not know you, before providing you with this access. We reserve the right to charge a nominal fee for such requests.

If there is a problem we may ask you to put your request in writing. If we cannot give you access, we will tell you within 30 days if at all possible and tell you the reason, as best we can, as to why we cannot give you access.

If you believe there is a mistake in the information, you have the right to ask for it to be corrected. This applies to factual information and not to any professional opinions we may have formed. We may ask you to provide documentation that our files are wrong. Where we agree that we made a mistake, we will make the correction and notify anyone to whom we sent this information. If we do not agree that we have made a mistake, we will still agree to include in our file a brief statement from you on the point and we will forward that statement to anyone else who received the earlier information.

DO YOU HAVE A QUESTION?
Our Information Officer, Chris Cole, can be reached at:

29 Noxon St. | Ingersoll, ON | N5C 3V6
PHONE (519) 485-4444

He will attempt to answer any questions or concerns you might have.

If you wish to make a formal complaint about our privacy practices, you may make it in writing to our Information Officer. She will acknowledge receipt of your complaint; ensure that it is investigated promptly and that you are provided with a formal decision and reasons in writing.

If you have a concern about the professionalism or competence of our services or the mental or physical capacity of any of our professional staff we would ask you to discuss those concerns with us. However, if we cannot satisfy your concerns, you are entitled to complain to our regulatory bodies:

COLLEGE OF PHYSIOTHERAPISTS OF ONTARIO
230 Richmond St. W., 10th Floor
Toronto, ON
M5V 1V6

COLLEGE OF MASSAGE THERAPISTS OF ONTARIO
1867 Yonge St., Suite 810
Toronto, ON
M4S 1Y5

This policy is made under the *Personal Information Protection and Electronic Documents Act*. That is a complex Act and provides some additional exceptions to the privacy principles that are too detailed to set out here. There are some rare exceptions to the commitments set out above. A copy of this document can be found on our website at www.activecarephysiotherapy.com.

For more general inquiries, the Privacy Commissioner of Canada oversees the administration of the privacy legislation in the private sector. The Commissioner also acts as a kind of ombudsman for privacy disputes. The Privacy Commissioner can be reached at:

112 KENT STREET | OTTAWA, ONTARIO | K1A 1H3
PHONE (613) 995-8210 | **TOLL-FREE** 1-800-282-1376 | **FAX** (613) 947-6850
www.privcom.gc.ca

Appendix

Table A1 – Disclosure without Consent

To whom disclosure must be made	**What information must be disclosed**	**Authority**
Aviation Medical Advisor	Information about flight crew members, air traffic controllers or other aviation license holders who have a condition that may impact their ability to perform their job in a safe manner	*Aeronautics Act*
Chief Medical Officer of Health or Medical Officer of Health	Information to diagnose, investigate, prevent, treat or contain communicable diseases	*Health Protection and Promotion Act* *Personal Health Information Protection Act*
Chief Medical Officer of Health or Medical Officer of Health or a physician designated by the Chief Medical Officer of Health	Information to diagnose, investigate, prevent, treat or contain SARS	*Public Hospitals Act*
Children's Aid Society	Information about a child in need of protection (e.g., abuse or neglect)	*Child and Family Services Act*

To whom disclosure must be made	**What information must be disclosed**	**Authority**
College of a regulated health care professional	Where there are reasonable grounds to believe a health care professional has sexually abused a patient, details of the allegation, name of the health care professional and name of the allegedly abused patient The patient's name can only be provided with consent You must also include your name as the individual filing the report.	*Regulated Health Professions Act*
College of a regulated health care professional	A written report, within 30 days, regarding revocation, suspension, termination or dissolution of a health care professionals' privileges, employment or practice for reasons of professional misconduct, incapacity or incompetence	*Regulated Health Professions Act*
College of Physicians and Surgeons of Ontario	Information about the care or treatment of a patient by the physician under investigation	*Public Hospitals Act* Notice must be given to the Chief of Staff and the administrator of the hospital

To whom disclosure must be made	**What information must be disclosed**	**Authority**
Coroner or designated Police Officer	Facts surrounding the death of an individual in prescribed circumstances (e.g., violence, negligence or malpractice) Information about a patient who died while in the hospital after being transferred from a listed facility, institution or home Information requested for the purpose of an investigation	*Coroners Act*
Minister of Health and Long-Term Care	Information for data collection, organization and analysis	*Public Hospitals Act*
Ontario Health Insurance Plan	Information about the funding of patient services	*Public Hospitals Act*
Order, warrant, writ, summons or other process issued by an Ontario court	Information outlined on the warrant, summons, etc.	*Personal Health Information Protection Act*
Physician assessor appointed by the Ministry of Health and Long-Term Care	Information to evaluate applications to the Underserviced Area Program	*Public Hospitals Act*
Registrar General	Births and deaths	*Vital Statistics Act*
Registrar of Motor Vehicles	Name, address and condition of a person who has a condition that may make it unsafe for them to drive	*Highway Traffic Act*

To whom disclosure must be made	What information must be disclosed	Authority
Subpoena issued by an Ontario court	Information outlined in the subpoena	*Personal Health Information Protection Act*
Trillium Gift of Life Network	For tissue donations or transplants purposes, notice of the fact that a patient died or is expected to die imminently (not in force yet)	*Trillium Gift of Life Network Act* Consent must be decided jointly with the Network to determine the need to contact the patient or substitute decision-maker
Workplace Safety and Insurance Board	Information the Board requires about a patient receiving benefits under the *Workplace Safety and Insurance Act*	*Workplace Safety and Insurance Act*

The following tables outline examples of where personal health information may be disclosed.

Table A2 - Disclosure for Health Related Programs and Legislation

Person requesting health record or patient information	Purpose	Consent Needed	Authority to release information
Ambulance services operator or delivery agent or the Minister	Administration/ enforcement of the *Ambulance Act*	No	*Ambulance Act*

Person requesting health record or patient information	**Purpose**	**Consent Needed**	**Authority to release information**
Cancer Care Ontario, Canadian Institute for Health Information, Institute for Clinical Evaluative Sciences or Pediatric Oncology Group of Ontario	To analyze or compile statistical information	No	Personal Health Information Protection Act regulations[†]
Chief Medical Officer of Health, Medical Officer of Health or a physician designated by the Chief Medical Officer of Health	To report communicable diseases	No	Health Protection and Promotion Act
College of Pharmacists Investigator	Administration/ enforcement of the Drug Interchangeability and Dispensing Fee Act	No	Drug Interchangeability and Dispensing Fee Act
College under the RHPA, or Social Work and Social Services Act, or Board of Regents under the Drugless Practitioners Act	Administration/ enforcement of the relevant statutes	No	Personal Health Information Protection Act

Person requesting health record or patient information	**Purpose**	**Consent Needed**	**Authority to release information**
Deputy Minister of Veteran's Affairs or person with express direction	To review the information about the care received by a member of the Canadian Armed Forces	No	Public Hospitals Act
Individual assessing patient capacity, who is not providing care to the patient	To assess capacity under the Substitute Decisions Act, Health Care Consent Act, or Personal Health Information Protection Act	No	Substitute Decisions Act; Health Care Consent Act; Personal Health Information Protection Act
Minister Inspector	Administration/ enforcement of the Public Hospitals Act	No	Public Hospitals Act
Minister Inspector	Enforcement of the Drugs and Pharmacy Regulation Act	No	Drugs and Pharmacy Regulation Act
Public Guardian and Trustee	To investigate an allegation that a patient is unable to manage their property	No	Public Hospitals Act; Personal Health Information Protection Act

Person requesting health record or patient information	**Purpose**	**Consent Needed**	**Authority to release information**
Public Guardian and Trustee, Children's Lawyer, Residential Placement Advisory Committee, Registrar of Adoption of Information, Childrens' Aid Societies	To carry out their duties and, for the PGT, to investigate serious adverse harm resulting from alleged incapacity	No	Personal Health Information Protection Act

Table A3 Disclosure to Lawyers, Insurance Companies, Adjusters, Investigators

Person requesting health record or patient information	Purpose	Consent Needed	Authority to release information
Lawyers, Insurance Companies, Adjusters on behalf of a patient	To assist a patient with a claim or proceeding	Yes	Express consent
Lawyers, Insurance Companies, Adjusters, Investigators on behalf of a third party, if the third party is an agent or former agent of the physician	To assist the third party with a proceeding	No	*Personal Health Information Protection Act*

Table A4 Disclosure to Legal Authorities and Law Enforcement

Person requesting health record or patient information	Purpose	Consent Needed	Authority to release information
Head of penal or custodial institution or an officer in charge of a psychiatric facility where the patient is being lawfully detained	To assist with health care or placement decisions	No	*Personal Health Information Protection Act*
Investigator or Inspector	To conduct an investigation or inspection authorized by a warrant or law	No	*Personal Health Information Protection Act*
Police without a warrant	Legal authorities and law enforcement	Yes	Express consent
Police without a warrant	Where there are reasonable grounds to believe that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm	No	*Personal Health Information Protection Act*

Person requesting health record or patient information	Purpose	Consent Needed	Authority to release information
Probation and Parole Services	Legal authorities and law enforcement	Yes	Express consent