

**Health
Claims for
Auto
Insurance
Processing**

Health Claims for Auto Insurance Processing ("HCAIP")

HCAIP Privacy Policy



Health Claims for Auto Insurance

1. DEFINITIONS: 3

2. EXECUTIVE OVERVIEW 5

3. PRIVACY PRINCIPLES..... 6

 Accountability: 6

 Identifying Purpose:..... 6

 Consent: 6

 Limiting Collection: 7

 Limiting use, disclosure and retention: 7

 Accuracy:..... 7

 Safeguards: 8

 Openness: 8

 Individual Access:..... 8

 Challenging Compliance:..... 9

4. DATA BREACH..... 9

5. DISASTER RECOVERY:..... 9

1. DEFINITIONS:

HCAI : Health Claims for Auto Insurance software and hardware system used to process claims data.

HCAIP: Health Claims for Auto Insurance Processing, the corporation overseeing HCAI.

HCDB: Health Claims Data Base is a database used by IBC to compile aggregate data on treatments and to investigate fraud.

PHI: *personal health information means identifying information about an individual in oral or recorded form, if the information,*

- (a.) *relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,*
- (b.) *relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,*
- (c.) *is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual,*
- (d.) *relates to payments or eligibility for health care in respect of the individual,*
- (e.) *relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,*
- (f.) *is the individual's health number, or*
- (g.) *identifies an individual's substitute decision-maker.*

Once this data is moved to HCDB, it cannot be attached to a specific person because the PI below, is removed. It is no longer considered to be personal health information.

PI: *"personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."* In the HCAI system this will be data that identifies a specific claimant like date of birth, policy number, diagnosis etc. This allows files to be accurately matched to the right person. Information is de-identified before health information is moved to HCDB. The provider information which includes name, place of work, identifying numbers is not considered PI.

PII: "personally identifiable information" any information which may be used to identify an individual and information about that identifiable individual. In HCAI policies this includes PI and PHI.

CI: Confidential Information includes PI, PHI and business information that is not openly available.

PIPEDA: Personal Information Protection and Electronic Documents Act (federal act)

PHIPA: Personal Health Information Protection Act (Ontario)

Facility: one or more health care professionals operating as a clinic or unit and submitting claims under one facility number

FSCO: Financial Services Commission of Ontario

De-identified Information: data that cannot be tied to a specific person, in the case of HCDB this means that the claimant cannot be identified from the available information.

Health Information Custodian: the health care facility that directly collects information from claimants.

Provider: health care professionals who are providing rehabilitation services to claimants, commonly Physiotherapists, Chiropractors, Occupational Therapists etc.

OCF: Ontario Claim Forms are standardized forms, regulated by law, which Providers use to submit information about claimants to the insurance adjusters. Claimants will be shown these forms as they need to be signed in order to give consent for submitting the information.

IBC: Insurance Bureau of Canada is a trade association for Canadian insurers; it is not an insurance company.

2. EXECUTIVE OVERVIEW

The insurance industry and FSCO realized that paper systems for submitting treatment plans are slow and potentially inaccurate. It also means that there is no reliable and complete collection of data with which to determine effective treatments for conditions following auto accidents.

Health Claims for Auto Insurance Processing (“HCAIP”) has been established as a not-for-profit corporation formed under the laws of Ontario to operate the Health Claims for Auto Insurance “HCAI” system.

Health Claims for Auto Insurance Systems (HCAI) is an electronic system for transmitting Ontario auto insurance health claims forms between Insurers and Health Care Facilities. It was developed in consultation with FSCO and other stakeholders in the auto insurance system, including various health care provider associations

HCAI accepts submission by Health Care Facilities on standard Ontario Claims Forms (OCF). These forms may be submitted electronically or in paper format. The data on the paper forms will be manually entered into the HCAI System, hence converting it to electronic format.

The HCAI system was designed to use a common framework for the collection of quality data and to streamline the exchange of information between automobile Insurers and Health Care Facilities.

For Insurers, HCAI ensures that the information collected about automobile-accident-related injuries and the proposed treatments is complete, consistent and reliable. This enables Insurers to make prompt, informed and fair decisions on medical and rehabilitation-related costs.

For Health Care Facilities, HCAI provides a method for the immediate and secure submission of accurate and complete data to Insurers. Facilities are also able to monitor an Insurer’s response to any of the submitted documents, in real time, and to manage their automobile-related accounts on-line.

HCAI improves the accountability of all parties, streamlines the process of delivering health care services to those injured in automobile accidents, and enhances communication among Insurers, Facilities and claimants.

HCAIP ensures that information processed and stored in HCAI is protected, regardless of the media or methods of transmission. In addition, access to PII is limited to those with a need to know.

All employees, contractors, consultants and vendors are required to sign confidentiality agreements before accessing PII or confidential information.

3. PRIVACY PRINCIPLES

Privacy laws in Canada are based on ten standard principles contained in the CSA Model Code for the Protection of Privacy. The following outlines how HCAIP implements these principles.

Accountability:

An organization is responsible for personal information under its control and shall designate a person who is accountable for the organization's compliance with the following principles.

The HCAIP Chief Privacy Officer is responsible for the corporation's compliance with the HCAIP Privacy Policy (this policy). This Officer is responsible for developing, implementing and auditing the privacy program as well as co-operating with the Privacy Commissioner should the occasion arise. This Policy applies guidelines to conform to federal and provincial privacy legislations.

Identifying Purpose:

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

HCAIP does not directly collect information from claimants but rather processes data that has been collected by Health Care Facilities (Information Custodians). This information is submitted on OCFs. Before or at the time of collection, the purpose is identified for the claimant by the Facility and documented. HCAI processes OCF-9s, -18s, -21s, and -23s. These forms may be viewed at www.hcaiinfo.ca

If PII is to be used for an un-identified purpose claimants will be contacted for signed consent before use, unless the information is required by law. This means that if HCAIP is presented with a properly executed legal request for information, it will be released.

Consent:

The knowledge and consent of the individual are required for the collection, use or disclosure of personal information except where inappropriate.

HCAI relies on Health Care Facilities to obtain consent as required by Privacy laws.

At the time of collection or before submission to HCAI the Facility/Provider is required to inform the claimant of the purpose and use of their information. OCFs contain written notice requiring the claimant's signature. The facility must ensure the claimant understands how the PII will be collected, disclosed and used.

Health Care Facilities will collect and keep on file consents provided by claimants. In the unusual circumstance where HCAI collects consent it will be explicit (written).

Limiting Collection:

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

The OCFs have been designed to collect only necessary data which is submitted to HCAI. The facility is responsible for completing and submitting only the required OCFs and containing only the required information.

Limiting use, disclosure and retention:

Personal information shall not be used or disclosed for purposes other than for those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

HCAI does not use the PII received, rather facilitates communication of data between Health Care Facilities and Insurers.

1. HCAIP does not disclose identifiable data to third parties unless required by law. HCAIP does provide data to the IBC HCDB which has been de-identified except for the claimant name. See IBC Privacy/Security policy at www.abc.ca for information on use, disclosure and retention.
2. PII is retained in HCAI for one year from last activity. Paper OCFs will be entered into the system then destroyed as soon as the form is deemed to be complete and accurate in its electronic form.
3. Retention guidelines comply with all regulations and upon reaching the expiry date paper will be shredded and electronic data will be permanently erased.
4. Audit trails of all access to data are maintained as long as the data is maintained.

Accuracy:

PII shall be as accurate, complete and up to date as is necessary for the purposes for which it is to be used.

Health Care Facilities are responsible for ascertaining the accuracy of data before submission. Best practices are in place to ensure data submitted on paper is transposed accurately. Should a claimant find an error in their data, HCAIP will determine where the error was made and take appropriate steps to have it corrected. Tracking history will be in place to record events around the change.

Safeguards:

Personal information is protected by security safeguards appropriate to the sensitivity of the information.

1. The security safeguards protect information against loss, theft, unauthorized access, disclosure, copying, use or modification. This applies to PII regardless of the format in which it is kept.
2. Electronic data is encrypted and access to identifiable data is strictly limited to those with a need to know. Access to identifiable data is tracked.
3. Data is destroyed following industry best practices available for the media involved.
4. Business Continuity Plans are developed and maintained.

Openness:

HCAIP shall make readily available to individuals specific information about its policies and practices related to its handling of PII.

HCAI shall post on its' website the privacy policy. The policy or more detailed information will also be available by verbal or written request to the Chief Privacy Officer.

Individual Access:

Upon request, an individual shall be informed of the existence, use and disclosure of personal information about the individual and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Individuals may request an accounting of their data, its use and disclosure and may challenge its accuracy.

In most instances requestors will be referred back to the collector of the information however, in the appropriate circumstance HCAIP will release the information

HCAIP will make the process for requesting access available to individuals and upon following the process, which includes proof of identity, the individual will be given a copy of their information. The information will be provided in an easily understandable form with any acronyms or insurance lingo explained. HCAIP must block access to information about third parties that may be part of the record.

HCAIP will notify the originating Insurer or Health Care Facility of any challenge and request they make the necessary changes and submit a corrected OCF. Any information under challenge will be flagged; changes will be tracked and upon resolution flagged as resolved.

Should the change request be denied, the claimant may file a letter of dispute and HCAIP will flag the file appropriately and notify the affected parties. For example, if the dispute is over the opinion expressed by a Provider (which cannot be changed), the members of the treatment team will be advised as necessary. The nature of the challenge will also be noted in the file.

Challenging Compliance:

An individual shall be able to challenge compliance with the above principles with the person who is accountable within the organization.

An individual shall be able to present a challenge concerning compliance, with the foregoing principles to the HCAIP Chief Privacy Officer. The Chief Privacy Officer will have access to senior management, legal and the HCAIP Board, as needed, to resolve the complaint. If the individual is not satisfied with the decision of the Chief Privacy Officer they will be informed of their right to appeal to the Office of the Federal Privacy Commissioner and contact information provided.

4. DATA BREACH

Should identifiable data be disclosed to unauthorized parties, data owners shall be informed of the incident as soon as possible if there is a possibility of harm. All instances of breach will be thoroughly investigated by HCAIP and measures put in place to prevent reoccurrence. The appropriate Privacy Commissioner will be informed as required by law.

Employees, contractors or consultants proved to be the cause of a breach shall be disciplined appropriately.

5. DISASTER RECOVERY:

In the event of a disaster occurring at the HCAI processing or data base location, Disaster Recovery Plans are in place to allow a smooth and rapid restoration of processing operations. The plans will be tested on a regular basis to ensure completeness and accuracy.

HCAIP Chief Privacy Officer
2235 Sheppard Avenue East
Atria II, Suite 1100
Toronto, ON M2J 5B5
Phone: 416-644-3120
Fax: 416-644-3121
privacyofficer@hcaiprocessing.ca