

Did you know?

In order to perform its function as an electronic interface between insurers and health care facilities, the HCAI system contains sensitive *“personal health information” (PHI)* and *“personally identifiable information” (PII)*. Protecting this information is the responsibility of HCAI Processing, health care staff, insurer personnel and claimants.

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

- i. relates to the physical or mental health of the individual, including information that consists of the health history of the individual’s family;
- ii. 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;
- iii. is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual;
- iv. relates to payments or eligibility for health care in respect of the individual;
- v. 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;
- vi. is the individual’s health number, OR
- vii. identifies an individual’s substitute decision-maker.

PII: “personally identifiable information” is any information which may be used to identify an individual and information about that identifiable individual.

Presently, all IBC-HCAI staff are contractually excluded from the authorized users of the HCAI production environment. In other words, any and all the PHI and PII that is entered into and/or contained in the HCAI production environment *is off-limits for IBC-HCAI staff*. This policy is under review and may change.

For now, however, IBC-HCAI staff must comply with the existing privacy constraints. PHI and PII should *not* be sent to HCAI staff as part of a request for assistance. Please ensure that all staff—including Managers, Adjusters, Technical Support and Administrators—are aware of this requirement. Sending PHI or PII through email or fax will result in the immediate notification of the HCAI Processing Privacy Officer; the Insurer’s own Privacy Officer will also be contacted. We ask that you please ensure all staff have reviewed the Insurer Privacy FAQs on the following page (which are also found in the Privacy section of www.hcaiinfo.ca).

HCAI Insurer Privacy FAQs

1. When is HCAI Processing (HCAIP) responsible for the confidentiality of PII and when is the insurer responsible?

HCAIP is responsible for PII while it is in the HCAI system. The insurer is responsible while it is being viewed on the monitor, printed, copied electronically, or filed in paper format.

2. What are the most important steps in keeping electronic HCAI data confidential?

- i. Have a secure password which you do not share!
- ii. Do not copy data to an unencrypted device.
- iii. Do not take screenshots/XML snippets containing PHI or PII and forward to HCAI Staff.

3. What do I do if I see inappropriate or unnecessary data (HCN, driver's license number etc.) in the free form field?

Contact the provider who has completed the OCF and request that they remove it. This type of identifying information is not necessary to the claim and should not be in a field where it might be seen by someone who has access only to anonymized data.

4. What do I do if I unintentionally share PII with someone not authorized to view it? (sharing data with IT or HCAI in order to gain assistance with an issue, for example)

Report to your Privacy Officer (PO). Even if you feel it is safe because it is someone in your organization who must maintain confidentiality, report it. It is the only way the PO will know if there needs to be additional steps taken to protect the data, a change in process to be considered or additional company-wide training.

5. What do I do if I think my password has been compromised?

Change it immediately and report to your organization's PO. In case it was an attempt to fraudulently access data the PO will need to investigate.

6. If a client suspects a breach and contacts HCAIP what will happen?

Usually the first step will be to contact the PO for the organization that collected the information. If the issue seems to be with the HCAI system then the HCAIP PO will pull the audit trail for that client's forms. The complainant will be given a list of the departments or organizations that have accessed the forms. If there is strong evidence that PII was compromised within the HCAI system names may have to be released. This will happen in very rare cases and only after legal consultation.

7. Do I still follow my organization's Privacy Policies and Processes?

Yes, it is your organizations policies that govern how you protect data. In many cases your policies will be stricter, and in all cases, more specific to your organization and your role. Although HCAIP is responsible for all data in the HCAI system, it is your PO who is responsible for data about your clients throughout the time they are insured by you.