Insurer User Manual

Chapter 11:

Security and Privacy

Table of Contents

Chapter 11: Security and Privacy

HCAI takes privacy and security seriously. It's at the forefront of everything we do to develop and operate HCAI. We play an active role in safeguarding the security of all forms submitted via HCAI as well as assessing the impact of programs and upgrades prior to being designed and implemented.

HCAI users play an essential role in preventing breaches and securing sensitive information. This chapter discusses security and privacy in the HCAI system.

Privacy and Security in HCAI

The Personal Information Protection and Electronic Documents Act (PIPEDA) legislates how organizations that hold Personal Information (PI) must operate. It describes how organizations are able to collect, use and disclose information. Further, they determine that all PI must be:

- Accurate;
- Secured;
- Accessible for inspection and correction purposes;
- Collected with consent and for a purpose that is reasonable; and
- Disclosed and use for the purpose for which it was obtained

HCAI is subject to the requirements set out in PIPEDA. HCAI employs multiple technologies and security practices to ensure the protection of the data entrusted to it, as described below.

Security

Secure hosting facility

The HCAI infrastructure is housed in secure hosting facilities. Access to the HCAI data is restricted to authorized personnel for the purposes of maintaining the system and that access is logged.

Application log-in

HCAI has been designed so that only authorized users can access the information in the system. All users must enter a valid user name and password to log in to the HCAI system. To maximize the security of every password, HCAI requires that they must:

- Contain at least eight characters
- Contain at least one uppercase character, lowercase character, numeral, and symbol (symbols are characters not defined as letters or numerals, such as @, #, $ and !)
- Not contain the user's actual name, user name or either of these spelled backwards
- Be changed every 90 days

As an additional security measure, if a user fails to provide the valid password for the same user name three times, the user will be suspended. Only a person with the Insurer User Administrator role in HCAI can reset the password once the password has been suspended.

Client Digital Certificates

Digital certificates are electronic credentials that connect the identity of the certificate owner to a pair (public or private) of electronic keys that can be used to sign information digitally. These electronic credentials make sure the keys actually belong to the person or organization specified.

HCAI integration web services (such as data feeds and extracts) use digital certificates for authentication of remote machines. Certificates are authenticated, issued and managed by a trusted third party called a certification authority (CA).

Certificates are issued to all parties authorized to use HCAI web services to send or receive data extracts. Insurer users using the web application do not require a digital certificate. They sign in to the HCAI web application with a user name and password. The digital certificates are installed on the insurer's integration service, which presents the certificate each times it connects to HCAI. Each digital certificate includes identification information about the connecting party and this information is the basis for authentication.

Insurer users with the Report Viewer role can request an Integration Activity Report in the 'Reports' tab. This report provides a log of all the activities done using an insurer's credentials over the integration channel for feeds and extracts. For more information on the Integration Activity Report, please review *Chapter 14: Insurer Reports*, which is available on the IBC Member Site. To request a user ID and password to access the member site, please submit a request to memberservices@ibc.ca.

HCAI helpdesk and administrator users

HCAI users performing either helpdesk or administrative tasks use the web login to access the system. Access to the system by application support staff is limited to a certain range of IP addresses, known to belong to authorized sources. This offers an additional layer of security, ensuring that these privileged accounts are restricted to only those individuals authorized by HCAI.

Web Services Authentication Errors

HCAI integration web services authenticate the remote machine's information for each request message. If a requesting user cannot be authenticated, the system displays a Simple Object Access Protocol (SOAP) security error page.

Authorization

HCAI enforces the specified security requirements by controlling user access to actions and data using a role-based authorization framework. A user is permitted to perform a certain action or view a certain piece of information based on their role (a set of permissions necessary for a user to perform their job) and their domain (the specific insurer with whom the user is associated).

Users are assigned one or more roles that represent the operations they are allowed to perform in the system. A role contains one or more tasks. Tasks are the individual actions required to do a specific piece of work. Roles, and the tasks that are associated with them, define the range of actions that a user can perform. For example, one user may be able to match claimants to a claim but not allowed to view or record decisions against the OCFs. This may be further qualified by specifying for which branch/claim group the user is allowed to perform the matching task. As mentioned above, this is accomplished by creating a domain, or organizational location, and limiting the user to operating within the domain.

HCAI domains, like role, are specified at the user level. Users may be assigned one or more domains. For example, while a senior manager might have access to an entire organization, a branch/claim group manager might be allowed access to only one branch/claim group.

Users will have access only to the organizations with which they are associated. This is managed by an HCAI organization administrator (within each insurer) using HCAI's inherent authorization functionality. No insurer will have access to another insurer's information unless it is configured as an authorized company, as in a parent-child company relationship.

Authorization configuration

Each insurer organization must assign a designated administrator who is responsible for maintaining the organization's user information and authorization details. Administrators assign roles and domains to users, specifying what they can do in the system.

It is the responsibility of the insurer organization to ensure that users are given access only to information they are legally entitled to access.

HCAI limits authorization configuration permissions to the domain of the administrator. This means that an administrator within a particular organization is able to assign permissions only to users associated with that organization.

Logging

Logging is the process of capturing and recording the significant actions performed by a user on the system, so that these actions can be reviewed and analyzed for security, privacy or other purposes.

The HCAI application has stringent logging requirements because the system manages the personal health information of individual claimants. Access to this information is rigorously controlled. Every attempt to access personal health information is recorded in audit logs.

Audit logs contain the following information:

- The identity of the user who performed the operation;
- The time of the activity;
- The type of activity, such as 'Invoice submitted' or 'Claim viewed'; and
- The entity upon which the activity was performed, such as "OCF-21" or "OCF-23".

Audit Data Retrieval

Privacy laws require that personal and personal health information be made available to individuals within 30 days of a request. HCAI is capable of providing the information necessary in order to comply with requests from individuals pursuant to existing privacy legislations.

Archiving

HCAI includes processes for automatically archiving data. Specific conditions must be satisfied before any HCAI data can be archived.

The below sections outline the business rules that apply to archiving documents in HCAI.

To qualify for archiving,

- All plans and invoices for a specific claimant are treated as a single "OCF Group";
- All plans and invoices related to the same claimant are archived at the same time;
- Every plan and invoice in the OCF group must be adjudicated; and
- one year must pass since the last adjudicated date for any plan or invoice in the OCF group.

As noted in *Chapter 5: Common Functionality*, archived OCFs are accessible through the HCAI web application via the OCF Document search feature

Privacy and Security Practices

HCAI has developed a comprehensive privacy and security program to guide employees, contractors and third parties in maintaining the confidentiality of PI and PHI. A Privacy and Information Security Officer has been appointed to oversee, update and implement the program as well as acting as a resource to users.

HCAI facilitates the transmission of data between insurers and providers and does not collect the PI or PHI. For this reason, HCAI depends on the privacy and security practices of its users to protect data when it is being entered into the system or is copied or stored outside the system.

HCAI expects users to be aware of their company's privacy and security practices that:

- Outline your responsibility to protect the PI and PHI of your claimants;
- Ensure that the authorizing officer is familiar with the HCAI application and that access to users in your organization is provided on a role-based model; as staff moves or leaves access is promptly changed or removed;
- Comply with the requirements as set out in agreements signed with HCAI;
- Explain appropriate file access for your role;
- Protect PI from unauthorized disclosure in paper, electronic or verbal format;
- Ensure claimant data is captured as accurately as possible to facilitate proper document matching;
- Establish retention, storage and destruction guidelines for data not in the HCAI system;
- Ensure your staff has privacy/security training on a regular basis and that changes in the HCAI system are communicated in a timely manner;
- Ensure that downloading claimant data to a hard drive or mobile device is prohibited unless known to a supervisor;
- Outline the process in the case of a privacy breach in your organization.

Chief Privacy and Information Security Officer
HCAI Processing
Fax: 416-644-3121
E-mail: privacyofficer@hcaiprocessing.ca