



Health Claims for Auto Insurance

FACILITY WEB MANUAL

September 2009

CHAPTER 1

Authorizing Officers (AO) & Personal Health Information

Do Not Proceed Until You Have Read This Section

Responsibility of the Authorizing Officer: Protect the Privacy of Your Patients, Clients and Professional Staff

When a health care facility (HCF) enrolls in HCAI, a responsible individual (called the Authorizing Officer) in that business (practice/clinic) will be given a unique username and password (a user profile). This user profile is comparable to a set of electronic **master keys to the clinic**, which permit access to all of the clinic's treatment records, including personally identifiable information (PII) and personal health information (PHI).

HCAI User Profile =



Set Up Written Privacy Procedures for Your Practice

All HCFs are required by privacy laws to have privacy procedures in place to secure the confidentiality of PII and PHI.

It is the responsibility of the Authorizing Officer (AO) to:

- Inform clinic personnel that user profiles (usernames and passwords) must not be shared.
- Understand the process by which user profiles are created.
- Monitor who is given a user profile (access to the “keys” to the HCF) and what levels of access are assigned.
- Ensure that access is removed when staff members leave the HCF or when their roles within the HCF change.
- Ensure procedures are put in place to:
 1. Assign user profiles to others in the HCF.
 - a. The AO may want to delegate the responsibility of assigning user profiles and the role of adding/removing providers to another person. **The AO should not share his or her password.**
 - b. To delegate user and provider management to another person, the AO must set up a user profile that has:
 - i. Facility level of access, including
 1. Facility Administrator (FA) role; and/or
 2. User Administrator (UA) role.
 - c. Once the other person has been set up with this user profile, she or he will be able to:
 - i. Add/delete providers as they join/leave the practice;
 - ii. Add/remove users to permit other staff to access the Web application for completion of forms or other activities;

Source: Health Claims for Auto Insurance Processing

- iii. Modify provider profiles (e.g., add professional designations, correct names, update registration numbers); and
 - iv. Modify user profiles.
 2. Inform and update staff on the roles of:
 - a. Facility Administrator
 - i. Change facility information such as email addresses, phone numbers and addresses; add new health providers; deactivate health providers who leave the practice; and correct health provider information.
 - b. User Administrator
 - i. Set up new users, deactivate users who leave the HCF or whose roles change within the HCF, and reset passwords for users.
 3. Inform staff members to approach the UA if they require a password reset.
 4. Inform the FA of his or her responsibility to:
 - a. Add new providers to be associated with the HCF, which includes obtaining an HCAI Provider Agreement form; and
 - b. Remove associated providers when they no longer work for the HCF. While the HCF may wish to keep a copy of the HCAI Provider Agreement form, the original should be given to the departing provider.
 5. Inform the UA of her or his responsibility to:
 - a. Deactivate user profiles when personnel change roles or leave the HCF; and
 - b. Manage password resets for users in the HCF.

Users, including the Authorizing Officer should not share passwords. All users should ensure their passwords are known only to them. (Remember, a username and password are like keys to the clinic and clinical records.)

Passwords and Logging On to the HCAI Application

HCAI has been designed so that only authorized users can access information in the system. HCAI uses a unique username and password for authentication. This is to protect PII and PHI and to secure the privacy of patients/clients/claimants.

All users must enter a valid username and password to log in to the system. To maximize the security of every password, HCAI requires that they:

1. Contain at least six characters;
2. Contain at least one character from three of the following four groups (a to d) and do not contain the letters described in e:
 - a. Uppercase characters
 - b. Lowercase characters
 - c. Numerals
 - d. Symbols (characters not defined as letters or numerals, such as @, !, #); and
3. Not contain the user's actual name, username, or either of these spelled backwards.
4. As an additional security measure, if a user fails to provide the valid password for the same username three times, the username will be suspended. Only a facility's User Administrator can reset it.

Password Maintenance

- All users should design a password they can easily remember. Refer to the Privacy FAQs at www.hcaiinfo.ca to learn how to design an effective password.
- It is not recommended that passwords be written down. If this is unavoidable, the password should not be stored near the computer(s).
- Usernames and passwords must not be shared.

Avoid Being Locked Out

To avoid getting locked out of the application:

- Take your time when logging on to HCAI.
- **If you enter the wrong password two times, do not try again.** Instead, click on the link “Forgot Your Password.”
- A new password will be emailed to the email address specified on your user account.

Figure 1.1 – Forgot Your Password?

The screenshot shows the HCAI Sign-In page. At the top left is the HCAI logo with the text 'Health Claims for Auto Insurance'. Below the logo is a 'HCAI Sign-In' header. To the right of the header is a 'Test HCAI' button. The main content area is divided into two columns. The left column contains a welcome message: 'Welcome to the HCAI application for automotive insurance health claims. Please enter your user name and password to sign-in:'. Below this are two input fields: 'User Name:' and 'Password:'. A blue 'SIGN-IN' button is positioned below the password field. Below the button are three links: 'Sign-in help', 'Forgot your password' (which is highlighted with a red rectangular box), and 'Register a facility'. The right column contains a text box with the following text: 'Health Claims for Auto Insurance (HCAI) is an initiative of Ontario auto insurers. It was developed in consultation with a number of stakeholders in the auto insurance system, including various health care provider associations. For more information about this initiative please visit [HCAI information site](#).' At the bottom of the page is a footer with the text: '© 2007 Health Claims for Auto Insurance Processing | [Privacy Policy](#)'.

Locked Out? Need a Password Reset?

- If you enter the wrong password or username three times in a row, you will be locked out and will require a password reset.
- Password resets can be done internally by facility User Administrators to whom the AO has assigned a User Administrator role. Refer to Chapter 3 of the HCAI Web User Manual to learn more about different user roles.
 - Note: User Administrators have authority to add and deactivate users (which is comparable to handing out and retrieving electronic keys to the practice). This is an important role in the HCF and should be assigned to someone with appropriate authority.
- All staff should be aware of individuals in the practice who have the User Administrator profile.
- See Chapter 3 to learn how a password reset is done.

Deciding Who Should Have a User Profile at the Health Care Facility

A “user” is someone who has been assigned a unique username and password, which can be used to enter the HCAI Web application. Each health care facility will have at least one user (initially that user will be the Authorizing Officer), and in many cases, more than one user will be desired.

When the facility is activated, only the Authorizing Officer (AO) will have a user profile. The AO will need to determine:

- a. Whether additional user profiles are needed;
- b. Who in the practice should receive a user profile (i.e., a unique username and password); and
- c. The level of access or permissions that will be made available to any new users.

Who Is a User?

A user is anyone with a unique username and password (i.e., a user profile). A user may be:

- Anyone associated with the facility that is involved in the creation, printing, reviewing, saving and/or submission of OCFs.
- Anyone who is responsible for managing your business (e.g., tracking health providers, following up with insurers about OCFs or receivables).
- A non-health professional or a health professional (provider).

TIP: Document your current process for the creation of OCFs. This will help you decide who may need a user profile.

Example – Pre-HCAI Procedure:

1. New patient arrives.
2. Receptionist obtains patient information, diagnosis and claim identifiers. New patient chart is created.
3. Patient is assigned to treating therapist and blank OCF 18 or 23 is assigned to treating PT.
4. Treating therapist completes handwritten OCF 18 or 23.
5. Handwritten OCF 18 or 23 is reviewed by PT with patient and handwritten copy is signed by patient.
6. OCF 18 or 23 is signed by treating PT.
7. Member of clerical staff faxes form to insurance adjuster.

Example – Post-HCAI Procedure (*with HCAI-related procedures in red*):

1. New patient arrives.
2. Receptionist obtains patient information, diagnosis and claim identifiers. New patient chart is created **and receptionist creates draft OCF 18 or 23 in HCAI.**
3. Patient is assigned to treating therapist and blank OCF is assigned to treating PT.
4. Treating therapist completes handwritten OCF 18 or 23.
5. Handwritten OCF 18 or 23 is reviewed by PT with patient and handwritten copy is signed by patient.
6. Handwritten OCF 18 or 23 is signed by treating PT.¹
7. Member of clerical staff **enters data into HCAI exactly as it appears on paper OCF.** Select “Yes” for questions “Is health practitioner signature on file?” and “Is claimant signature on file?”
8. Member of clerical staff **submits form via HCAI** to insurer. **HCAI document number confirming receipt by insurer is generated automatically.**

In the example above, the receptionist and/or clerical staff are engaged in OCF creation; therefore, your facility may wish to assign reception and clerical staff user profiles so they can log on to HCAI and create

¹ A hard copy of the signed form must be filed at the clinic and be available for audit purposes.

and/or submit OCFs. While in the example above the treating PT does not require a user profile, it is an option if the PT prefers to create OCFs online rather than on paper.

What Levels of Access Can a User Have?

Refer to Chapter 3.

How Can Departing Providers Ensure Their Names and Registration Numbers are Deactivated by a Facility?

- To confirm that a provider's name has been deactivated, the provider may request to be present when the facility's User Administrator deactivates his or her name.
- In addition, the provider may request receipt of the original copy of the Provider Agreement, which she or he signed upon becoming associated with the facility.
 - Without the HCAI Provider Agreement, the HCF has no authorization to use the provider's name or registration number in new treatment proposals (for future treatment) or to invoice for services delivered after the provider's last day of service.
 - Even if the provider has withdrawn the HCAI Provider Agreement form, the HCF may invoice for services delivered prior to the provider's last day at the HCF (i.e. when the Provider Agreement was still in force).

If this is not possible, and a provider has evidence about unauthorized use of his or her name and registration details, he or she may place a request with HCAI's Privacy Officer, who may agree to investigate whether the health professional's name and registration number are active with the HCF.

Draft Plans/Invoices and Personal Health Information

The information in the "draft" form will be visible to others at the facility.

- In order to ensure confidentiality of personal health information and your patients'/clients' rights to privacy, it is advisable that certain personal identifying information (PII) not be used on the draft form.
- The patient's actual name, date of accident, address, etc., may be inserted just before the form is submitted to the insurer, and the submitted form will not be visible to all in the facility.
- In the meantime, users must be able to identify which draft forms belong to an individual user (or health provider) who is working on the form and, also, which draft form is associated with which patient.
- To accomplish this, it is recommended that a draft form naming convention be developed within each facility to protect personal health information (PHI) while still enabling users to identify the draft forms on which they are working.