



How do I set up Medicare Australia Online Claiming in Best Practice?

This FAQ is intended to answer common questions about how to configure Best Practice to use Medicare Australia Online Claiming (MAOL).

Preparation

Please ensure that the server and all workstations are using BP version 1.7.0.500 or higher and have a working internet connection.

Best Practice has implemented the following components of Medicare Online:

- Online Bulk Bill Claiming (Medicare & Streamlined DVA)
- Online Patient & Veteran Verification
- Patient Claim Store & Forward
- ACIR Notification

Specialist and Allied Health claims are now supported.

For Medicare claims, all Allied Health items listed in the MBS Schedule GROUP M3 - ALLIED HEALTH SERVICES can be transmitted.

For DVA claims, the following Allied Health items can be transmitted:-

- Chiropractors
- Clinical Counsellors / Psychologists
- Community Nursing
- Dentists
- Diabetes Educators
- Dieticians
- Exercise Physiologists
- Occupational Therapists
- Optical dispensers
- Optometrists (includes Hardware)
- Orthoptists
- Osteopaths
- Physiotherapists
- Podiatrists
- Social Workers
- Speech Pathologists



BEFORE YOU BEGIN



Important: If you are currently using another Management package that uses Online Claiming, you will need to finalise and receipt all claims in that package before configuring BP for Online Claiming as Medicare Online Claiming can only operate from one software package at a time.

Refer to the FAQ document [BPM_FAQ-Moving to BPM from another Package.pdf](#)

All practitioners wishing to use Medicare Australia Online (MAOL) will need to register and obtain Medicare Site certificates. Please contact Medicare eBusiness centre on 1800 700 199 to obtain the relevant application forms.

- If you are already registered but are using another management package, you can use your current certificates to set up Medicare Online in BP but you will still need to notify Medicare so that they can change their system to indicate that you are now using Best Practice.
- If you are not currently registered, you will need to register and apply for a Medicare Site Certificate.
- Each time you add a new doctor to the practice, you will have to notify Medicare to add this doctor.

When completing the form you will need to provide your practice's Minor Id. This Minor ID Number is an 8 digit number derived from your Best Practice Site ID.



- 1) Identify your Site ID. Select 'Help' > 'About' from the main Best Practice screen. Your Site ID is displayed in the bottom left of the screen.
- 2) Take your BP Site ID and prefix it with the letters 'BPS'
- 3) Pad the ID with zeros so that the total length is 8 characters.

Examples:

If your Best Practice Site ID is 849, your Medicare Minor ID number would be BPS00849

If your Best Practice Site ID is 1234, your Medicare Minor ID number would be BPS01234



Setting up Online Claiming

To turn on Online Claiming in Best Practice, select **Setup > Configuration** from the main Best Practice screen. Scroll down to **Online claiming** and the following screen will be displayed.

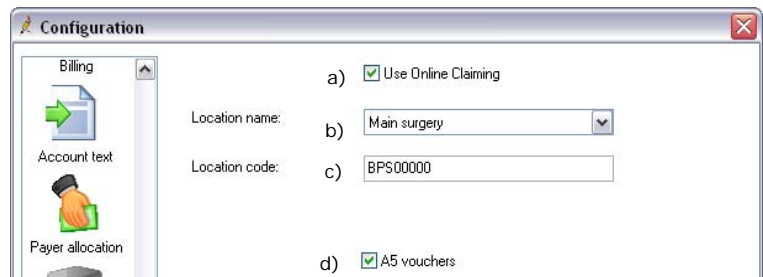
a) Click the check box **"Use Online Claiming"** to activate its use. When Online Claiming has been turned on, extra buttons and menu items become available within the Best Practice program.

b) **Location name** – you must select the Main Surgery location. Best Practice does not currently support MAOL for multiple locations.

c) **Location code** – this code is supplied to you by Best Practice Software. This is an 8 character number, prefixed by BPS and suffixed by your BP site ID number, then

padding between with zero's to make up the 8 characters. If you are unsure of your Best Practice site ID select **Help > About** or email sales@bpssoftware.com.au (e.g. Site 123 uses BPS00123).

d) **A5 Vouchers** – click this checkbox to print the Medicare and DVA vouchers as two separate A5 pages. If not selected, the two copies will be printed side by side on a single A4 page.



Certificate Management

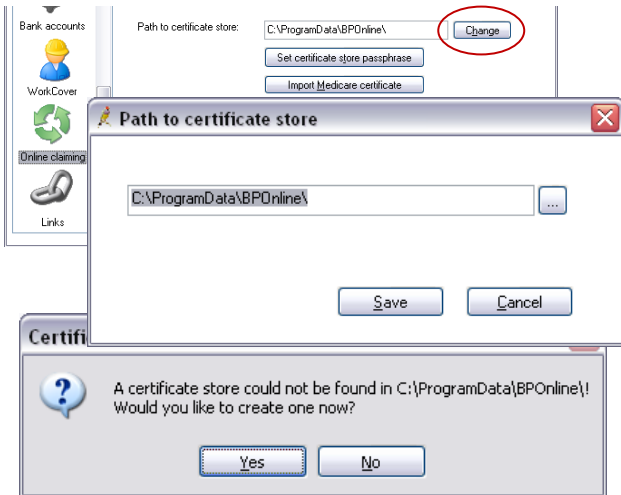
Medicare Australia's Online Claiming requires a HeSA Location Certificate to digitally sign data that is sent to Medicare. Medicare's HeSA public keys are used to encrypt the data. The HeSA PKI components are automatically installed by the Best Practice installer.

Configuring the Server

e) **Path to Certificate Store** – the certificate store is created on the server and then shared and used by all workstations where transmission to Medicare is to occur.



Note: This path is where Best Practice will store the certificates after they are imported using the 'Import Medicare Certificate' and 'Import site certificates' buttons. **DO NOT COPY your Certificates into this folder.**




There will only be **one** certificate store for the clinic. On the server the path **must** be set to c:\Program Data\BPOOnline\. (DO NOT CHANGE THIS PATH ON THE SERVER).

Click the 'Change' button to display the 'Path to Certificate Store' screen. The path c:\Program Data\BPOOnline\ will be displayed. Click the 'Save' button. You will be prompted to say that the certificate store does not exist and 'Would you like to create one now?'

Answer 'Yes' to create the store file.

You will then be prompted for a password for the certificate store. This password **MUST** be the same as the password provided to you from Medicare with your certificates. This is called your Personal Identification Code (PIC) code.

 **Information:** Do not misplace this password. You are responsible for this password; we cannot retrieve this for you.



f) Certificate Store Passphrase

This function would only be used if you need to 'reset' the passphrase for some reason. It **MUST** always remain the same as the one provided to you by Medicare.

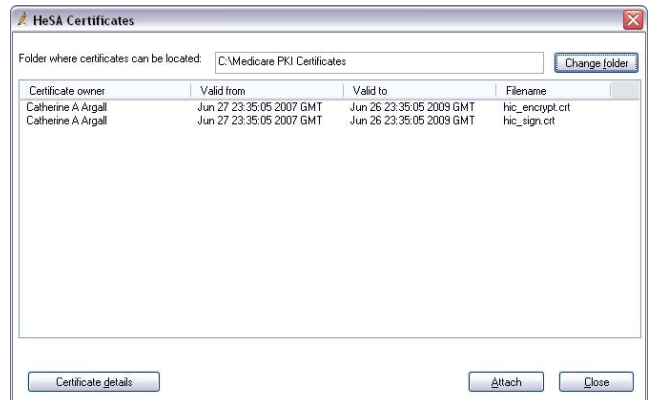
g) Import Medicare Certificate

These are the Medicare's HeSA public keys is used to encrypt the data

Click the "Import Medicare certificate" button to import the Medicare Australia public key. The HeSA Certificates screen will appear.

Medicare usually provides these certificates on a CD. Put this disk into the drive and click the "Change folder" button to navigate to the CD / DVD drive and click **OK**. (If the certificates have been copied to a folder on the server then navigate to this folder and click Ok).

If it has successfully found certificates, they will appear showing the 'Valid from' and 'Valid to' dates. There should be 2 certificates and usually the Certificate Owner will be 'Catherine A Argall' or 'Medicare Australia' and the file names should be 'hic_encrypt.crt' and 'hic_sign.crt'.



Highlight the first certificate and click 'Attach' to import them into the certificate store. The system will display a message when it has been imported. Repeat for the other certificate that is displayed.



h) Import site certificates

This function allows you to import the HeSA Location Certificate which is the practice's certificate to digitally sign data that is sent to Medicare.

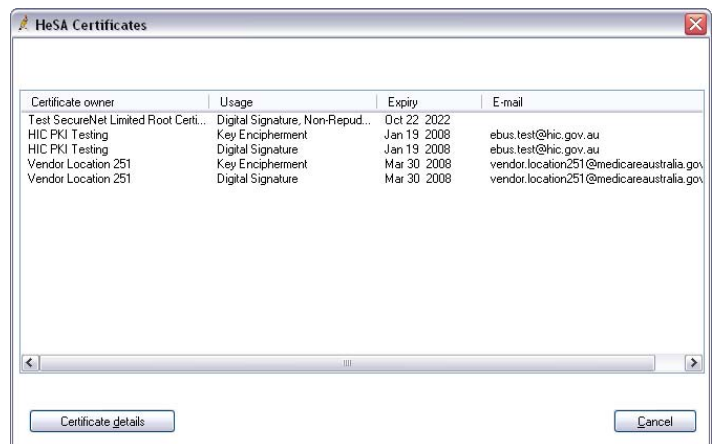
Click on the **'Import Site certificates button'**. The HeSA Certificates screen will appear. It should have remembered the path that you entered earlier but if not, click



on the **'Change folder'** button and browse to the location of the certificates. It should now display any site certificates found in that location. There should be 2 certificates, called **'fac_encrypt.p12'** and **'fac_sign.p12'**. Highlight the first file displayed and click the **'Attach'** button. The system will display a message when it has been imported. Repeat for the other certificate displayed. **'trust.p12'** cannot be attached and will produce a message stating this if an it's attempted.

i) Check certificate expiry

You should now check that the certificates imported are showing on the **'Check certificate expiry'** screen. Click the **'Check certificate expiry'** button.



There should be at least 5 items listed similar to those on the example below however two should mention 'Catherine A Argall' or 'Medicare Australia' in the Certificate owner column (these are Medicare Australia's certificates) and two should mention the clinic name. Check that all the 'Expiry' dates are future dates. Press **'Cancel'** to exit from this screen.

Press the **'Save'** button when you are back on the **'Configuration'** screen to save these changes.

Test the Link to Medicare

Before sending your first batch we suggest that you test the link to Medicare. Select **'View' > 'Patients'** from the main Best Practice screen.

Select a patient name and click **'View details'**. Click the **'Medicare / DVA eligibility check'** button at the bottom of the screen. This will contact Medicare and check whether the Medicare No is valid for this patient. If the communication is working correctly it will display a message such as the one shown.



If this test is successful, you should now configure each of your workstations to access the Medicare certificate store (see notes following on performing this step).

If this test is not successful please contact Best Practice support via phone or email **'support@bpsoftware.com.au'** to diagnose the problem.



Configuring the Workstations

- a) Exit from Best Practice on the Server.
- b) Browse to the folder **C:\ProgramData\BPOnline** on the server and 'share' the folder across the network. Once it is shared you will also need to give all users 'full control' permissions to the folder and its contents. Browse to the file '**HIC.psi**' and ensure that all users have 'full control' permission to this file.
- c) Go to the first workstation. Ensure that version 1.7.0.500 or higher has been installed and that when it was installed the '**Install Best Practice Software Online Claiming Module**' tick box was selected. You can tell whether this was done as there will be a folder C:\ProgramData\BPOnline on that workstation. If this folder is not found on the workstation you should apply the latest program update that matches the version on the server. Ensure that you tick the 'Online Claiming box' when it appears.
- d) Log into Best Practice.
- e) Select '**Setup**' > '**Configuration**' > '**Online Claiming**'. Tick the box 'Use Online Claiming', ensure that the Location Name says 'Main Surgery' and the Location code has been entered.
- f) **Path to certificate store:** - Click the change button and either type in the UNC path to the certificate store on the server (e.g. <\\servername\BPOnline>) or browse to this folder.
- g) **Check certificate expiry:-** Click on the '**Check certificate expiry**' button. If the sharing has been set up correctly for the certificate store the system will display the certificates and their expiry dates.
- h) **Check link to Medicare:** Follow the steps outlined in the '**Test the Link to Medicare**' section above to confirm that the workstation can communicate to Medicare.

You will now need to repeat this process on all workstations on the network.

We now recommend that you create an Online batch with just a few transactions and transmit this. Once this is successful you can create larger batches for transmission.

Vivas / ACIR Register



Important: This process must be done before proceeding.

Each time an immunisation is recorded for a child, a record is written to the VIVAS/ACIR register. If you have been using Best Practice for a while and transmitting the data via another application you should clear out this register **prior** to your first Online transmission from Best Practice. This can be done by selecting **Utilities > Vivas/ACIR** from the main Best Practice screen. Highlight all records to be deleted and select **File > Exclude Current Record**.

Alternatively, if you wish to have a hard copy of the records you can select **File > Print** and print the list. Once the printing is complete, you will be prompted '**Do you want to mark these immunisation records as notified to VIVAS**'. Answer 'Y' to mark all records and remove them from the list.

MORE INFORMATION

For more information consult the Best Practice Help Library or contact us via:



07 4155 8800



07 4153 2093



support@bpsoftware.com.au



<http://forum.bpsoftware.com.au>



<http://www.bpsoftware.com.au>



sales@bpsoftware.com.au

Last Reviewed: 11/12/2009