Public Private Interface (PPI) System
User Guide
for
Private Medical Record Officers

Revision 1.12

Prepared by:
AIS / AI3 Team
Information Technology Division
22 Jun 2011
## Amendment Log

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Version No.</th>
<th>Date of Amendment</th>
<th>Prepared by</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td></td>
<td>21 Mar 2006</td>
<td>IS1 team, ITD, HA</td>
<td>New document.</td>
</tr>
<tr>
<td>1.1</td>
<td></td>
<td>19 Dec 2006</td>
<td>IS1 team, ITD, HA</td>
<td>UI enhancement of Quick Access and Next Patient Button</td>
</tr>
<tr>
<td>1.2</td>
<td></td>
<td>26 Feb 2007</td>
<td>IS1 team, ITD, HA</td>
<td>UI Enhancement of Logon Page</td>
</tr>
<tr>
<td>1.3</td>
<td></td>
<td>24 Oct 2008</td>
<td>IS1 team, ITD, HA</td>
<td>Online activation</td>
</tr>
<tr>
<td>1.4</td>
<td></td>
<td>4 Feb 2009</td>
<td>IS1 team, ITD, HA</td>
<td>Address Searching function in User Account Management</td>
</tr>
<tr>
<td>1.5</td>
<td></td>
<td>30 June 2009</td>
<td>IS6 team, ITD, HA</td>
<td>System Requirement and Installation Guide</td>
</tr>
<tr>
<td>1.6</td>
<td></td>
<td>7 Oct 2009</td>
<td>IS6 team, ITD, HA</td>
<td>Change eHealth Logo</td>
</tr>
<tr>
<td>1.7</td>
<td></td>
<td>2 Mar 2010</td>
<td>IS6 team, ITD, HA</td>
<td>Updated Section 2.2 for HD PPP &amp; PEP</td>
</tr>
<tr>
<td>1.8</td>
<td></td>
<td>6 Jul 2010</td>
<td>AI3 team, ITD, HA</td>
<td>Updated Section 2.2 for SCP</td>
</tr>
<tr>
<td>1.9</td>
<td></td>
<td>24 Aug 2010</td>
<td>AI3 team, ITD, HA</td>
<td>Smart ID Enrollment</td>
</tr>
<tr>
<td>1.10</td>
<td></td>
<td>27 Oct 2010</td>
<td>AI3 team, ITD, HA</td>
<td>Add Section 5.2.5 for Reprint Consent Form function and Section 6 Reporting</td>
</tr>
<tr>
<td>1.11</td>
<td></td>
<td>26 May 2011</td>
<td>AI3 team, ITD, HA</td>
<td>Updated Section 5.2 for Smart ID Enrollment</td>
</tr>
<tr>
<td>1.12</td>
<td></td>
<td>22 Jun 2011</td>
<td>AI3 team, ITD, HA</td>
<td>Add Section 3.7. Update Section 3.4 and 4 for MUR Enhancement</td>
</tr>
</tbody>
</table>
Table of Contents

1. INTRODUCTION ........................................................................................................... 4
   1.1 ABOUT THIS MANUAL ................................................................................................. 4
   1.2 WHERE TO GET HELP ................................................................................................. 4

2. SYSTEM REQUIREMENT AND INSTALLATION GUIDE .................................................. 5
   2.1 HARDWARE REQUIREMENT ....................................................................................... 5
   2.2 SOFTWARE REQUIREMENT ....................................................................................... 5
   2.3 SYSTEM CONFIGURATION ....................................................................................... 6
       2.3.1 Printing ................................................................................................................ 6

3. SECURITY INFORMATION AND GUIDE TO USER LOGIN ........................................... 9
   3.1 GENERAL SECURITY INFORMATION ........................................................................ 9
       3.1.1 Access Control ........................................................................................................ 9
       3.1.2 User Account ......................................................................................................... 9
       3.1.3 Activity Logging .................................................................................................... 9
       3.1.4 Patient Consent ..................................................................................................... 9
   3.2 SYSTEM REQUIREMENTS ON PASSWORD MAINTENANCE .................................... 10
       3.2.1 General Guidelines ............................................................................................... 10
       3.2.2 Mandatory requirement on Password format ...................................................... 10
       3.2.3 Password Changes ............................................................................................... 10
       3.2.4 Password notification .......................................................................................... 11
   3.3 SECURITY TOKEN DEVICE ....................................................................................... 11
   3.4 LOGIN TO THE PPI-EPR SYSTEM ............................................................................ 12
       3.4.1 Login for the First Time ....................................................................................... 14
       3.4.2 Login successful .................................................................................................. 16
       3.4.3 Login with Replacement Security Token ............................................................. 18
       3.4.4 Login Failure and Automatic Lock-out ................................................................. 19
       3.4.5 Login through internal site .................................................................................. 19
   3.5 LOGOUT PPI-EPR SYSTEM ...................................................................................... 20
   3.6 RETURN TO MAIN MENU ....................................................................................... 20
   3.7 SWITCH ROLE .......................................................................................................... 21

4. UPDATE OWN PROFILE AND PASSWORD ..................................................................... 23
   4.1 UPDATE OWN PROFILE ............................................................................................ 23
       4.1.1 Update Personal Information .............................................................................. 23
       4.1.2 Update Role Information .................................................................................... 24
   4.2 CHANGE YOUR OWN PASSWORD ............................................................................ 26

5. PATIENT ENROLLMENT AND PATIENT PROFILE MAINTENANCE ............................... 27
   5.1 PATIENT ENROLLMENT ............................................................................................ 27
   5.2 SMART ID ENROLLMENT ......................................................................................... 29
       5.2.1 Enrollment with Smart ID .................................................................................... 29
       5.2.2 Non-smart ID Enrollment with 2D barcode pre-filled form .................................. 36
       5.2.3 Non-smart ID Enrollment with hand written consent form ................................ 41
       5.2.4 Print Patient’s Access Key (For Private Hospital Only) ......................................... 44
       5.2.5 Reprint consent form function ............................................................................. 46
   5.3 UPDATE PATIENT’S PERSONAL INFORMATION ..................................................... 47

6. REPORTING ....................................................................................................................... 49
   6.1 VIEW REPORT LIST .................................................................................................. 49
1. Introduction

The Public Private Interface / electronic Patient Record Sharing Pilot System (PPI-ePR) is a web-based application aiming at improving the sharing of patient’s clinical information between public and private healthcare providers to facilitate a seamless and better quality healthcare environment for patients upon patient’s consent.

The Hospital Authority (HA), being the largest healthcare provider in Hong Kong, has collected clinical data on patients under its care through its integrated clinical information system over the past years and established a patient-centered, lifelong longitudinal clinical data repository, namely the electronic-Patient Record (ePR).

A pilot for this collaborative project is to be launched by 1Q 2006, in which HA will share the ePR of patients who are under the care of selected private healthcare providers upon patients’ consent. Through this pilot run, it aims to establish & assess the logistics involved, and to determine the key success criteria and identify critical components for the provision of a community-wide health information portal in the future.

1.1 About this manual

This manual aims at providing users with a quick and working reference of the PPI-ePR system and includes the following 4 sections:

1. System Requirement & Installation Guide
   This section describes the hardware & software requirement and the setup procedure before accessing the PPI-ePR system.

2. Security Information and Guide to User Login
   This section describes the security features of the system and how to use security token to login to the PPI-ePR system.

3. Guide to use the functions provided by PPI-ePR
   This section describes the various functions provided by the PPI-ePR system.

1.2 Where to Get Help

If you require help with the use of the PPI-ePR system, please contact the system administrator of your hospital. If you do not have a system administrator, please contact the Hospital Authority PPI-ePR Program Office on 2300-6654, or via email to the following addresses:

Internet: ppi.epr@ha.org.hk
Intranet: HO PPI-ePR Program Office (hopsoppiepr@ho.ha.org.hk)
2. System Requirement and Installation Guide

The minimum hardware and software requirement for your computer system to access the PPI system is described below.

2.1 Hardware Requirement

- IBM Compatible PC (Pentium and above) with a minimum of 256 MB RAM, or
- Intel-based Mac (either desktop or laptop) with a minimum of 1GB RAM
- Broadband Internet access

2.2 Software Requirement

For Microsoft Windows:
- Microsoft Windows 2000 with SP4 or above OR Windows XP with SP1 or above OR Windows Vista
- One of the following web browser installed:
  - Microsoft Internet Explorer version 6 with SP1 or above
  - Microsoft Internet Explorer version 7
  - Mozilla Firefox 3.x
- Adobe Acrobat Reader Version 5.0 or above. You can download a free copy of the current version of Adobe Acrobat Reader at [http://www.adobe.com/](http://www.adobe.com/)

For Mac:
- MacOS X 10.4 (Tiger) or 10.5 (Leopard)
- Web browser: Safari 3.x
- Adobe Acrobat Reader for Mac version 8 or above. You can download a free copy of the current version of Adobe Acrobat Reader at [http://www.adobe.com/](http://www.adobe.com/)

Note that Primary Care Profile (PCP) can only run on Internet Explorer version 6/7 under current implementation.

Browser-Applications support matrix:

<table>
<thead>
<tr>
<th></th>
<th>Internet Explorer 6/7</th>
<th>Firefox 3.x</th>
<th>Safari 3.x on Mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePR</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Primary Care Profile (PCP)</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Cataract Profile</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Haemodialysis Public-Private Partnership Programme (HDPPP)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Patient Empowerment Profile (PEP)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
2.3 System Configuration

Before you access the PPI system, you should configure your computer as specified below.

2.3.1 Printing

If you need to print reports or letters through the system, please set up your Internet Explorer as follows:

1. Open your Internet Explorer.
2. Click <File>, and then <Page Setup>.
3. Clear the contents in the <Header> and <Footer> sections as below.
4. Click <OK> button to save the changes.
Mozilla Firefox

1. Open your Firefox browser

2. Click <File> and then click <Page setup>

3. Set all headers and footers to "-blank-":
Safari (for MacOS X)

Uncheck the `<Print headers and footers>` option every time when you print a document in Safari.
3. Security Information and Guide to User Login

3.1 General Security Information

3.1.1 Access Control

Access to the different functions in the PPI-ePR system is granted based on the job duties of each user. If you think that your type and level of access in the PPI-ePR system do not match your responsibilities, please contact your PPI-ePR system administrator or the Hospital Authority PPI-ePR Program Office.

3.1.2 User Account

You are assigned a unique User ID (Login ID) when granted access to the PPI-ePR system for your sole and personal use only. For HA users, you are required to login to the system using the correct User ID and Password. For non-HA users, a Security Token is also provided and you are required to login to the system using the correct User ID, Password and the Security Code as displayed on the Security Token at the time of logging in.

Access to the system is restricted to authorised users only and you must not share your User ID, Password and Token to others. Please refer to the ‘IT Security Guide for the PPI-ePR Project’ for good security practices. A copy of which has been distributed to you when your account was created or you can download a copy from the PPI-ePR web site.

3.1.3 Activity Logging

The PPI-ePR system logs every user activity (e.g. accessing patient’s clinical data, create an account) in the system automatically for audit purposes. The logged information includes the access date/time, User ID, type of transaction, the record and data fields accessed, and if any data is changed, the before and after image of the change. This logging allows the system administrator to trace every action within the system to the individual user and you will be personally responsible for the actions logged with your User ID.

You should use the PPI-ePR system to perform your duties in relation to patient care and related purposes only according to the Terms and Conditions of this website. Regular audit reports on individual users’ activities in the PPI-ePR system will be generated for monitoring by the system administrators at the Hospital Authority and each participating Private Hospitals.

3.1.4 Patient Consent

You are allowed to access the patients’ records only when the patient has consented. Apart from the system logging, the PPI-ePR system will generate a SMS message to the patient’s mobile phone every time a patient’s record is opened in the PPI-ePR system. The message contains the time and name of the user accessing his / her record so that the patient can report any unauthorised access to the Hospital Authority immediately.
3.2 System requirements on Password Maintenance

3.2.1 General Guidelines

Passwords are the principal means of authenticating the user and validating a user’s authority to access the system. You are advised to adopt the following guidelines to protect your password so as to protect your own user account.

1. Keep passwords confidential. Do not disclose your password to others to prevent unauthorised access using your account.
2. Avoid keeping a paper record of passwords.
3. Change passwords whenever there is any indication of possible system or password compromise.
4. Change passwords at regular intervals (about 30 days) and avoid reusing or "cycling" old passwords.
5. Avoid basing passwords on any of the following:
   - months of the year, days of the week or any other aspect of the date
   - family names, initials or car registration numbers
   - the organisation names, identifiers or references
   - telephone numbers (or similar all-numeric groups)
   - User ID, user name, group id or other system identifier
   - more than two identical characters
   - words that can be found in dictionaries

3.2.2 Mandatory requirement on Password format

The system will automatically check the format of your password when you create a new password. Passwords of the following format will be rejected:

- with length less than 8 characters
- with the user’s User ID or HKID embedded in the password
- with 3 or more consecutive identical characters in the password
- with the word ‘password’ embedded
- same password as your previous password

3.2.3 Password Changes

The system requires you to change your password upon successful login under the following circumstances:

- login for the first time
- login after your password has been reset
- login after your password has not been changed for a period of times
The following page will be displayed when the system requires you to change your password. You must change your password successfully before you can proceed to other functions when this page is displayed. When you change your password, please note the mandatory requirement on the format of the password as described in section 3.2.2.

In addition, you can change your password any time via the Update Own Profile function in the PPI-ePR.

### 3.2.4 Password notification

When your account is created or when your password is reset, an e-mail from ppi.epr.system@ha.org.hk will be sent to you to advise you of your password. It is therefore very important that you should keep your updated e-mail address recorded in the PPI-ePR system. Your User ID will be sent to you in a separate e-mail. You should memorise your User ID and password on receipt of the e-mails and destroy them immediately. If you forget your password, you have to call your system administrator or the PPI-ePR Program Office to reset your password. Since the password is system generated and no one knows your password, it is impossible to revert your password to a previous password.

### 3.3 Security Token Device

A Security Token Device as shown below will be assigned to each user who has to access the PPI-ePR via the internet. This device is not required for Hospital Authority users who only access the system within the HA network.

Internet users must have this token with him/her at the time of logging into the PPI-ePR system. The system requires internet users to enter the 6 digit code as displayed on the LCD screen of the Security Token device at logging in, e.g. 032848 as shown above.

The Security Code will expire within a short period of time and a new code will be displayed. You must input the Security Code as displayed on the Token at the time of logging in.
If you find any problem with your Security Token Device, please contact your system administrator or the PPI-ePR Program Office.

3.4 Login to the PPI-ePR System

1. Go to [http://ppi.ha.org.hk](http://ppi.ha.org.hk) with your web browser. The PPI logon screen will be displayed. Enter your User ID and click <Continue>.

2. **For HA users**, the following page will be displayed and you are required to enter your Password. Note that the password is case-sensitive. Please ensure that you have input your password with the appropriate case and check that Caps Lock is not accidentally kept on.
3. **For non-HA users** or users accessing the system via the internet, the following page will be displayed. You are required to input both the Password and the Security Code from your Security Token Device.

**Notes:**
- the password is case-sensitive. Please ensure that you have input your password with the appropriate case and check that Caps Lock is not accidentally kept on.
- if you are unsure of what is the Security Code, please refer to paragraph 3.3 above on Security Token Device.

4. Press the <Logon> button to proceed.
3.4.1 Login for the First Time

1. For non-HA users or users accessing the system via the internet, the following page will be displayed. You are required to input both the first 4 digit no. of your HKID (e.g. HKID:Z123456(7), input "1234") and the registered phone no to activate the account.

If you have input an incorrect HKID and / or registered phone no, the following page will be displayed. Please be aware that after a number of incorrect attempts to log on, we will disable online access by your User Account. Please contact your PPI-ePR system administrator or the Program Office to re-activate your account.
2. The first time when you login successfully to the system, a ‘Notice and Disclaimer for HA PPI-ePR Sharing Pilot Project’ will be displayed.

3. Please read through this important notice regarding the use of the PPI-ePR system and its site. The <Accept> and <Reject> button will be enabled when you scroll to the end of the notice.

4. If you do not agree with the disclaimer, click the <Reject> button. You will be logged out of the system and return to the login page.
5. If you agree with the disclaimer, click the <Accept> button. You will be asked to change your password. Input the new password twice and click the <Submit> button to confirm. You can click <Reset> to clear all entries.

3.4.2 Login successful

1. On successful login, and successful change of password (when required), the following page will be displayed.
2. Information on your last logon, including date, time and status (success/failure) will be displayed. You should check this information every time after you logon into the system to ensure that no unauthorised login attempts have been made using your User ID. If in doubt, you should contact your System Administrator or the Program Office for assistance.

3. Functions which are available to you are displayed on the <Menu Bar>. There are a total of 6 groups of functions offered by the system:
   - Patient Data Enquiry
   - Patient Enrolment
   - Reporting
   - Account Management
   - Update Own Profile

If you found that the functions displayed on your <Menu Bar> do not match your job duties, please contact your PPI-ePR system administrator or the Program Officer for support.
3.4.3 Login with Replacement Security Token (For users with security token)

1. For non-HA users or users accessing the system via the internet with replacement security token, the following login page will be displayed.

![Login with Replacement Security Token](image)

2. If you have input a security code generated by replacement security token device, the following page will be displayed. You are required to input both the first 4 digit no. of your HKID (e.g. HKID:Z123456(7), input "1234") and the registered phone no to activate the account.

![Activation of New Security Token](image)

**Notes:**
- If the input security code was generated by original security token, you can login successfully with normal flow. The replacement security token will only activate after new security code has been input.

3. On successful login, the following page will be displayed with message
"New token activated". The activate process is completed and the original security token is no longer valid for login into PPI-ePR System.

3.4.4 Login Failure and Automatic Lock-out

If you have input an incorrect User ID and/or Password and/or Security Code, the following Page will be displayed. Please be aware that after a number of incorrect attempts to log on, we disable online access by your User Account. Please contact your PPI-ePR system administrator or the Program Office to re-activate your account.

3.4.5 Login through internal site (For users with security token)

If you have both Internal and External roles, you still can use internal site for accessing the account. After entering the User ID and click <Continue>, there
is a check box "Not Applicable" next to Security Code Text box. If user just want to use internal roles, the user can check the check box "Not Applicable" and just fill in the Password and click <Logon> button to login the system. Be reminded that the user can only use the Internal Roles by using this login method. If you want to use the external roles, just fill in the Security Code and unchecked the check box "Not Applicable".

3.5 Logout PPI-ePR System

To logout from the system, click the <Logout> icon on the menu bar.

Notes:
- Remember to logout the system when you finish working with the system. Forgetting to logout the system may lead to your User ID being used to retrieve confidential information by unauthorised person.
- The system will automatically log you off if your account remains inactive within the system after a period of time. You will be required to login again after your session has been ‘timed-out’.
- It is a good practice that you should close a patient’s record immediately after your encounter with the patient. This will avoid the patient’s record being viewed by another patient or staff member.

3.6 Return To Main Menu

To return to the main page from any functions within the system, click the <Home> icon on the menu bar.
3.7 Switch Role

By using the switch role function, the user can switch the log-in role to the selected role.

1. You can see the current role on the left hand side of the header menu bar. Click the <Switch Role> button on the menu bar.

2. Click on the link of the role that you would like to change. You can check the "Default" check boxes next to the roles for setting the default role. Once the default role is set, the system will automatically log in the default role when logging in the system.
3. Enter the password and click <Continue> button.

4. Finally, the role is switched to the selected role.
4. Update Own Profile and Password

4.1 Update Own Profile

All users have permission to update their own information. Follow the steps below to update your own profile.

1. Click <Update Own Profile> on the Menu Bar, then click <Update Own Profile> on Sub-menu Bar.

4.1.1 Update Personal Information

1. Click the right top corner icon on the Personal Information Section to update the personal information.

2. Update the Information and Click <Save> button.
3. The Personal Information is updated.

4.1.2 Update Role Information

1. Click the icon besides the role you would like to edit
2. Update the Role Information. You can add or update the Institute Information by clicking the <add> or <edit> button in the Institute/clinic Information Section.

3. Fill in the Institution Information Form. Click <Confirm> button to save the changes. Click <Delete> button to delete the institutes. Click <Back> button to decline the changes.
4. Click <Save> to save the updated Role Information.

4.2 Change Your Own Password

1. Click <Update Own Profile> on the Menu Bar, then click <Change Password> on the Sub-menu Bar

2. Enter the old password and enter the new password twice and press <Save> button.

Notes
Please refer to ‘System requirements on Password Maintenance’ in the Chapter on ‘Security Information and Guide to User Login’ for guidelines on Password maintenance.
5. Patient Enrollment and Patient Profile Maintenance

There are two methods for patient enrollment.

Enroll New Patient (Section 5.1)

1. Click <Patient Enrollment> on the Menu Bar. Click <Enroll New Patient> on the Sub-menu Bar.

2. Enter the patient’s HKID, Sex, Name and Date of Birth and click the <Next> button.

Smart ID Enrollment (Section 5.2)
3. If the system finds a complete match of an existing HA patient with the four pieces of data entered, the following Patient Enrolment page will be displayed. Complete the details on the patient. Fields with an asterisk (*) must be completed and cannot be left blank.

4. **Important Notes on Patient’s Address**

   You must compare the <HKPMI Address> displayed on the screen with the patient’s reported address on the consent form. If the patient reports a different address from the one displayed, please input the reported address in the slot provided for <Address on Consent Form>.

   Please advise the patient that his/her registered address with the Hospital Authority (HKPMI address) will be used for all official correspondence from the HA to the patient regarding the PPI-ePR system. If the patient intends to use the address on the consent form as his/her correspondence address, he/she should provide address proof for this address and authorises the HA to update his/her registered address with the HA.

5. Click <Save> to confirm enrollment and <Back> to cancel.

   The following screen will be displayed upon successful enrollment. The patient will receive an ‘Access Key’ via a SMS message to his/her mobile phone. A letter of confirmation with detail information on the PPI-ePR system will be posted to the patient’s registered address with the HA.
5.2 Smart ID Enrollment

5.2.1 Enrollment with Smart ID

Before proceeding to Smart ID Enrollment, users should have Hong Kong Smart ID card reader and Java JRE installed into his/her computer. Please refer to "SmartID Card Reader and JRE Installation Guide" for installation.

1. Click <Patient Enrollment> on the Menu Bar. Click <Smart ID Enrollment> on the Sub-menu Bar.

2. Ask patient to insert the Smart ID card into the card reader.

3. Click <Start> under "Method 1: Smart ID Enrollment" to start Enrollment process.

If the following dialog box is prompted, Please click "Yes" to continue the patient enrolment by smart ID operation. PPI-ePR users are also advised to check the option “Always trust content from this publisher” to avoid repeated appearing of the dialog box.

Could be one of the following value, depending on the server used in current operation: id11.hcv.gov.hk, id12.hcv.gov.hk, id21.hcv.gov.hk
4. Click <Confirm> if patient agreed to gain access to the data stored in the Smart ID card.

The card holder has inserted the Smart ID Card and agreed to gain access to the data stored in the chip.

Confirm  Cancel

5. Remove Smart ID from card reader when complete.

Read Hong Kong Smart Identity Card

Please remove the Hong Kong Smart Identity Card from the smart card reader.
6. The following screen will be displayed. Specify sex of the patient.

![Patient Enrollment](image)

7. If the system finds a complete match of an existing HA patient, the following Patient Enrolment page will be displayed. Complete the details on the patient. Fields with an asterisk (*) must be completed and cannot be left blank.

![Patient Enrollment (SMART ID) - Step 1: Enter Patient's Information](image)
8. **Important Notes on Patient’s Address**

You must compare the `<HKPMI Address>` displayed on the screen with the patient’s reported address on the consent form. If the patient reports a different address from the one displayed, please input the reported address in the slot provided for `<Address on Consent Form>`.

Please advise the patient that his/her registered address with the Hospital Authority (HKPMI address) will be used for all official correspondence from the HA to the patient regarding the PPI-ePR system. If the patient intends to use the address on the consent form as his/her correspondence address, he/she should provide address proof for this address and authorises the HA to update his/her registered address with the HA.

9. Click `<Continue>` to verify patient information or `<Cancel>` to cancel enrollment without saving.

---

**Patient Enrollment (SMART ID): Step 2: Verify Patient’s Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKID</td>
<td>L104720(8)</td>
</tr>
<tr>
<td>Sex</td>
<td>Male</td>
</tr>
<tr>
<td>Name</td>
<td>GONG SUN AU YEUNG, SAU KUEN</td>
</tr>
<tr>
<td>DOB</td>
<td>08/10/1962</td>
</tr>
<tr>
<td>Contact Number</td>
<td>91234567</td>
</tr>
<tr>
<td>Email Address</td>
<td><a href="mailto:a@a.com">a@a.com</a></td>
</tr>
<tr>
<td>* Mobile</td>
<td>91234567</td>
</tr>
<tr>
<td>* Language for SMS</td>
<td>English</td>
</tr>
<tr>
<td>HKPMI</td>
<td>RM 345, 13/F, BLK B, TIGER HOUSE, ABC, CITY EIGHT, 100 ICE ROAD</td>
</tr>
<tr>
<td>* Address Matched?</td>
<td>Matched</td>
</tr>
<tr>
<td>Address on Consent Form (If different from HKPMI Address)</td>
<td>N/A</td>
</tr>
<tr>
<td>Clinic</td>
<td>Hong Kong Adventist Hospital</td>
</tr>
</tbody>
</table>

Click `<Continue>` to save changes or `<Back>` to return to the previous screen to update patient information.
10. The following screen will be displayed after verification.

Click <Print Application Form> to print the application form, ask the patient to tick the "agree" box and sign the form.
If any amendment is to be made on the form, click <Modify Entry> to update the information and reprint the form.

Click <Accept> if patient accept and sign the application form, or click <Decline> in case patient reject the application.
11. The following screen will be displayed upon successful enrollment. The patient will receive an ‘Access Key’ via a SMS message to his/her mobile phone. A letter of confirmation with detail information on the PPI-ePR system will be posted to the patient’s registered address with the HA.

**Patient Enrollment (SMART ID)** - Completed: Patient will receive the Access Key via SMS. Please print the confirmation letter and give to patient. Please fax the consent form to Programme Office (Fax: 2762-5802) and keep the original copy at local MRO.

Click < Print Confirmation Letter > to print the confirmation letter to patient. Close the confirmation letter after print out.
5.2.2 Non-smart ID Enrollment with 2D barcode pre-filled form

1. Click <Patient Enrollment> on the Menu Bar. Click <Smart ID Enrollment> on the Sub-menu Bar.

2. Enter the patient’s HKID, Sex, Name and Date of Birth and click the <Next> button.
3. If the system finds a complete match of an existing HA patient, the following Patient Enrolment page will be displayed. Complete the details on the patient. Fields with an asterisk (*) must be completed and cannot be left blank.

Select “Pre-filled form with 2D barcode” in Enrollment Form Type

Click <Continue> to verify patient information or <Cancel> to cancel enrollment without saving.
Click <Continue> to save changes or <Back> to return to the previous screen to update patient information.

4. The following screen will be displayed after verification.

Click <Print Application Form> to print the application form, ask patient to tick the ‘agree’ box and sign the form for signature.

If any amendment is to be made on the form, click <Modify Entry> to update the information and reprint the form.
Click **<Accept>** if patient accept and sign the application form, or click **<Decline>** in case patient reject the application.
5. The following screen will be displayed upon successful enrollment. The patient will receive an ‘Access Key’ via a SMS message to his/her mobile phone. Upon completion of vetting, a letter of confirmation with detail information on the PPI-ePR system will be posted to the patient’s registered address with the HA.

The screen for Private Organization

The screen for Private Hospital with printing access key function (Details please reference to section 5.1.4)
5.2.3 Non-smart ID Enrollment with hand written consent form

1. Click <Patient Enrollment> on the Menu Bar. Click <Smart ID Enrollment> on the Sub-menu Bar.

2. Enter the patient’s HKID, Sex, Name and Date of Birth and click the <Next> button

3. If the system finds a complete match of an existing HA patient, the following Patient Enrolment page will be displayed. Complete the details on the patient. Fields with an asterisk (*) must be completed and cannot be left blank.

Select “Hand written consent form” in Enrollment Form Type
**Patient Enrollment (Non-SMART ID): Step 1: Enter Patient's Information**

- **HKID**: B000000(0)
- **Sex**: Male
- **Name**: CHAN, SIU MING
- **DOB**: 01/01/1981
- **Contact Number**: 
- **Email Address**: 
- **Mobile**: 
- **Language for SMS**: English
- **HKPMI**: RM 890, GOOD HOUSE
- **Address Matched?**: Matched
- **Address on Consent Form (If different from HKPMI Address)**: 
- **Enrollment Form Type**: Pre-filled form with 2D barcode
- **Clinic**: Hong Kong Adventist Hospital

Click <Continue> to verify patient information or <Cancel> to cancel enrollment without saving.

**Patient Enrollment (Non-SMART ID): Step 2: Verify Patient's Information**

- **HKID**: B000000(0)
- **Sex**: Male
- **Name**: CHAN, SIU MING
- **DOB**: 01/01/1981
- **Contact Number**: 91234567
- **Email Address**: a@z.com
- **Mobile**: 91234567
- **Language for SMS**: English
- **HKPMI**: RM 890, GOOD HOUSE
- **Address Matched?**: Matched
- **Address on Consent Form (If different from HKPMI Address)**: N/A
- **Clinic**: Hong Kong Adventist Hospital

Click <Confirm> to save changes or <Back> to return to the previous screen to update patient information.
4. The following screen will be displayed upon successful enrollment. The patient will receive an ‘Access Key’ via a SMS message to his/her mobile phone. Upon completion of vetting, a letter of confirmation with detail information on the PPI-ePR system will be posted to the patient’s registered address with the HA.

The screen for Private Organization

Patient Enrollment (Non-SMART ID - Pre-filled form with 2D barcode) - Completed: Patient will receive the Access Key via SMS. Please collect and send the original application forms, as well as related supplementary documents to Programme Office by POST for vetting process.

The screen for Private Hospital with printing access key function (Details please reference to section 5.1.4)

Patient Enrollment (Non-SMART ID - Pre-filled form with 2D barcode) - Completed: Patient will receive the Access Key via SMS. Please collect and send the original application forms, as well as related supplementary documents to Programme Office by POST for vetting process.
5.2.4 Print Patient’s Access Key (For Private Hospital Only)

Under normal circumstances, the Access Key will be sent to the patient’s mobile phone immediately via a SMS message. It is therefore unnecessary to print or view the Patient’s Access Key via the system.

However, under very exceptional circumstances when the key is urgently required and the patient cannot receive the SMS message on the spot, you can print the patient’s Access Key with the patient’s consent by following the steps below. As the Access Key is a major security control to safe-guard the patient’s personal data, you must print the patient’s Access Key only when it is absolutely necessary.

1. Click the icon on the right hand side of the screen.

2. The following page will be displayed. You are required to input your User ID and Password again to ensure that you did not click on the Print Access Key icon by accident and to avoid future repudiation on your intention to print. Click <Submit> to continue or <Reset> to clear the entered data.
3. The patient’s Access Key will be displayed. Click <Print> to print the patient’s Access Key.
5.2.5 Reprint consent form function

1. Click <Patient Enrolment>, then click <Print Form>.

2. Enter the patient’s HKID No and click the <Next> button.

3. If the entered information is correct, the following page will be displayed and a pop up Application Form is shown. (Only for the Unvetted Patient enrolled by you and the enrolment method is either SmartID or 2D Barcode.)
5.3 Update Patient’s personal information

1. Click <Patient Enrolment>, then click <Update Patient Profile>.

   ![Patient Enrolment](image)

2. Enter the patient’s HKID No, Sex, Name & Date of Birth and click the <Next> button.

3. If the entered information is correct, the following page will be displayed and you can update the patient’s information as required.

   ![Update Patient Profile](image)
With the minor consent case patients, the following page will be displayed and click <Yes> to extend the minor consent case. New Access Key will be sent to the patient’s mobile phone immediately via a SMS message.

Click <Save> to save changes made and <Back> to return to the previous screen without saving.

4. The following screen will be displayed upon successful update of the changes. If required, you can follow the same steps as described in paragraph 5.2.42 to print the Patient’s Access Key.
6. Reporting

A number of reports are available to you for monitoring of exceptions or to facilitate regular auditing on the usage of the system. The types of reports available to you will depend on the access rights assigned to your account by your system administrator. Please contact your system administrator or the Hospital Authority PPI-ePR Program Office if you found that you need some of the reports which are not available to you.

The patient’s or user’s HKID number, name, address and other personal details will be listed on some reports. These reports will be marked ‘Confidential’ and you must secure these reports areas:

1. **Do not** print these reports unless it is absolutely required.
2. **Do not** leave the hard copy of these reports in areas which can be accessed by people who do not have the rights to view these reports.
3. **Do** lock away these reports securely if they are to be retained for filing / record purposes
4. **Do** dispose of unwanted print-outs properly in an appropriate manner (shredding, incineration, etc).
5. **Never** dispose these reports into rubbish bins with other waste paper.

6.1 View Report List

2. A list of reports belonging to the selected group will be displayed. Click on the *Report Name* to view the report.

![Image of list of reports]

- List of Unwetted Patients
- List of Expired Access Key
- List of Patient PII Address Changed

3. The selected report will be displayed. Click on the <Print Report> button to print the report.

![Image of printed report]

List of Unwetted Patients 7 days after enrollment

Print date: 07 Oct 2009