Framework for IT Deployment on Community Pharmacy Programme (Residential Care Homes)

Health Bureau

February, 2026

Content

1. Background

The Chief Executive's 2024 Policy Address announced the launch of the Community Pharmacy Programme (CPP), with the aim of implementing the recommendation of adopting a multi-disciplinary approach for the proper management of chronic diseases in the community as set out in the Primary Healthcare Blueprint (Blueprint). CPP aims at alleviating the burden on the public healthcare system while driving the sustainable development of the primary healthcare system through public-private partnership as well as enhancing the professional role of community pharmacists within the primary healthcare team.

The CPP will adopt two service models, namely the Community and the Residential Care Homes (RCH). The CPP(RCH) is expected to commence in phases starting from the first quarter of 2027. Under the CPP (RCH), HA-prescribed drugs will be regularly dispensed to HA patients residing in RCHs for the elderly and persons with disabilities to improve the current practice of daily drug sorting and distribution by RCH staff, with a view to enhancing patients' drug compliance and reducing the risks associated with overstocking of drugs. The services of the CPP (RCH) include drug dispensing, reconciling, and prepackaging of the daily required drugs. In addition, pharmacists will assist RCHs in adopting information technology for drug management to enhance drug safety in RCHs.

Apart from basic drug dispensing service, community pharmacies will also provide standard Value-added Services and non-standard Value-added Services that are proposed by the community pharmacies and accepted by the Government. As for the CPP (RCH), value-added services include multi-dose packaging for solid-oral medications, setup of electronic Medication Administration Record (eMAR) systems, drug management and storage at RCHs, health promotion and staff training programme, thereby ensuring safe and accurate drug administration, as well as enhancing drug safety in RCHs.

This document provides the framework for IT deployment for potential service provider's reference and is intended solely for the purpose of collecting market information. The Government may update this document from time to time. Neither this document nor any activities associated with it shall create any legal obligations or liabilities on the part of the Government. Furthermore, neither this document nor any of its contents shall form the basis of any contract or commitment whatsoever.

2. Service Scope

The Contractor shall provide partnered RCHs and Programme Patients with the following Services:

(a) Medication dispensing against HA electronic prescriptions with medication reconciliation

(b) Provision of Core Standard Value-added Services (VAS)* and elective Standard Value-added Services (VAS), if applicable

(c) Provision of Non-standard Value-added Services, if applicable

An overview of the workflow for the Services is set out in Appendix 1 to facilitate the planning of provision of the Services.

**Core Standard VAS shall be made available by the Community Pharmacy for procurement by partnered RCH*

3. Overview of the IT System

(a) The Contractor shall order Programme Drugs and submit claim for Monthly Dispensing Service Fee on the Government IT Platform.

(b) The Contractor shall have and deploy its own pharmacy operation IT system ("Pharmacy System") for carrying out the operation of the Services.

(c) The Contractor shall interface its Pharmacy System at its own costs with the Government IT Platform before the commencement of the Service Period.

(d) The Contractor shall access or retrieve the information specified by the Government, including but not limited to clinical data and prescription details, from the Government IT Platform and shall submit the information specified by the Government, including but not limited to dispensing data, clinical documentation and co-payment details, to the Government IT Platform while providing Services to partnered RCHs and Programme Patients. The Contractor shall ensure that the latest information is obtained before dispensing, and the design of Pharmacy System shall accommodate regular retrieval of updated data accordingly.

(e) The Contractor shall submit the documentation for Standard VAS performed by the Community Pharmacist to the Government IT Platform via the Pharmacy System according to IT requirement specifications in Appendix 3.

(f) The Contractor shall ensure that the Pharmacy System shall process the electronic prescriptions in accordance with applicable laws and regulations.

(g) The Contractor shall ensure there is reliable and secured internet access for eHealth access and the operation of the Services.

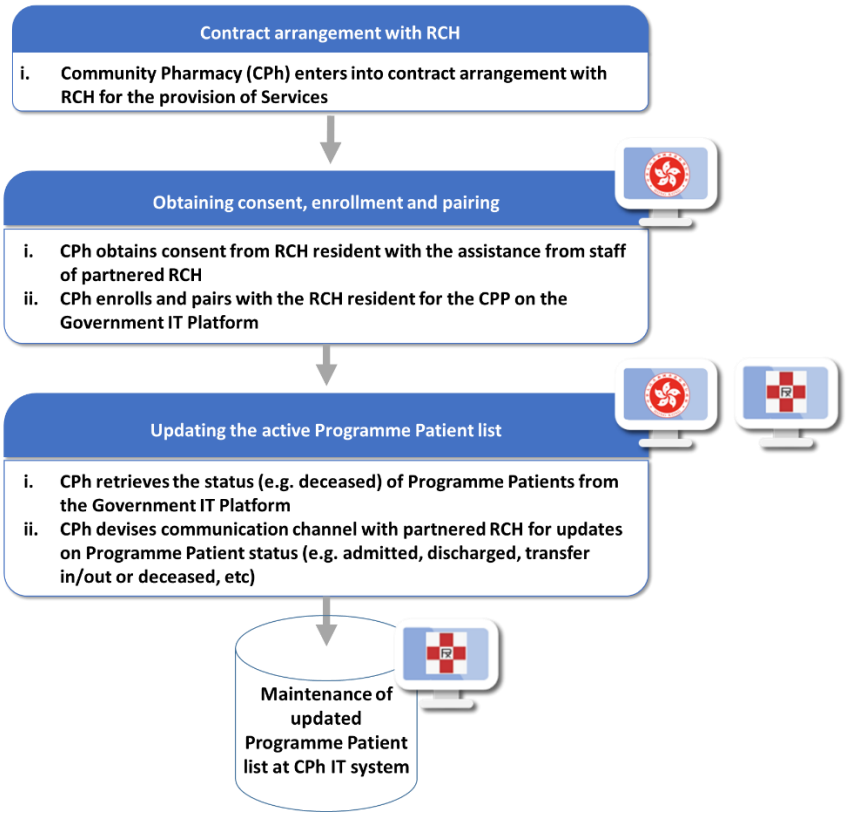
4. Readiness of the IT System

The Contractor shall fulfil the Provisions Relating to eHealth specified in Appendix 2 and IT requirements specified in Appendix 3 in terms of i) functional requirements; ii) security and network requirements; and iii) data interface and connectivity requirements, and shall ensure the Pharmacy System complete the interface testing successfully and fully functional within sixteen (16) weeks in accordance with the schedule in Appendix 4 after the Letter of Conditional Acceptance is issued.

Appendix 1 – Overview of the Workflow for the Services

The Service workflow is illustrated for reference only and may be updated from time to time by the Government.

I. Entering into contract arrangement with RCH and maintenance of updated Programme Patient list

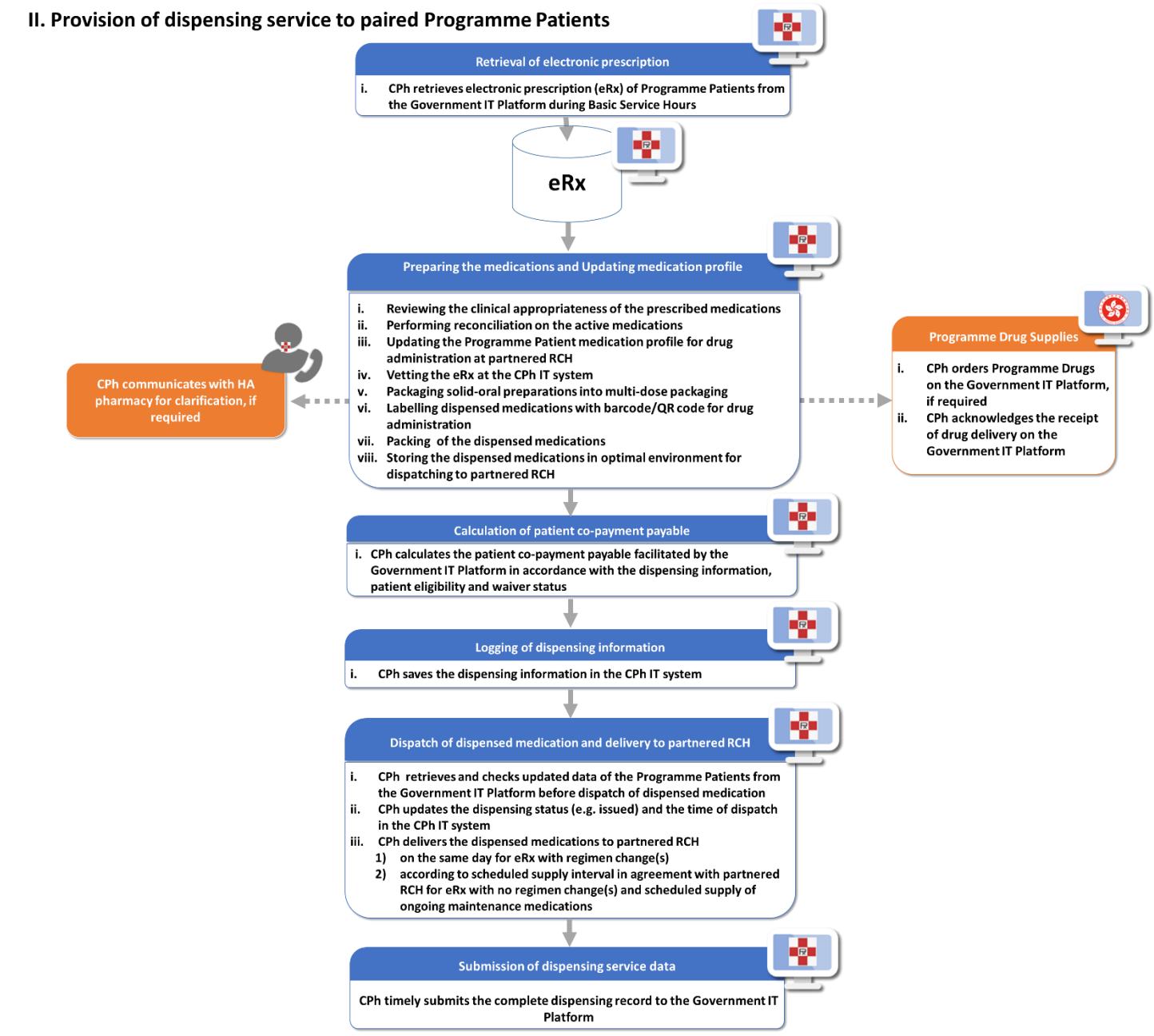


Task to be performed on the Government IT Platform

Task to be performed on the CPh IT System

The Service workflow is illustrated for reference only and may be updated from time to time by the Government.

II. Provision of dispensing service to paired Programme Patients



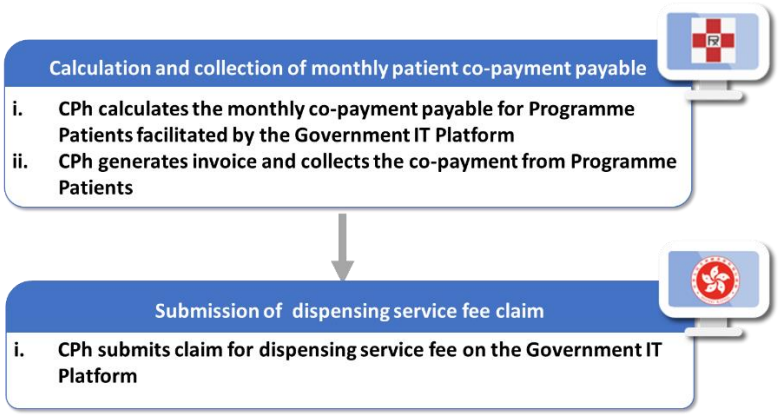
Task to be performed on the Government IT Platform

Task to be performed on the CPh IT System

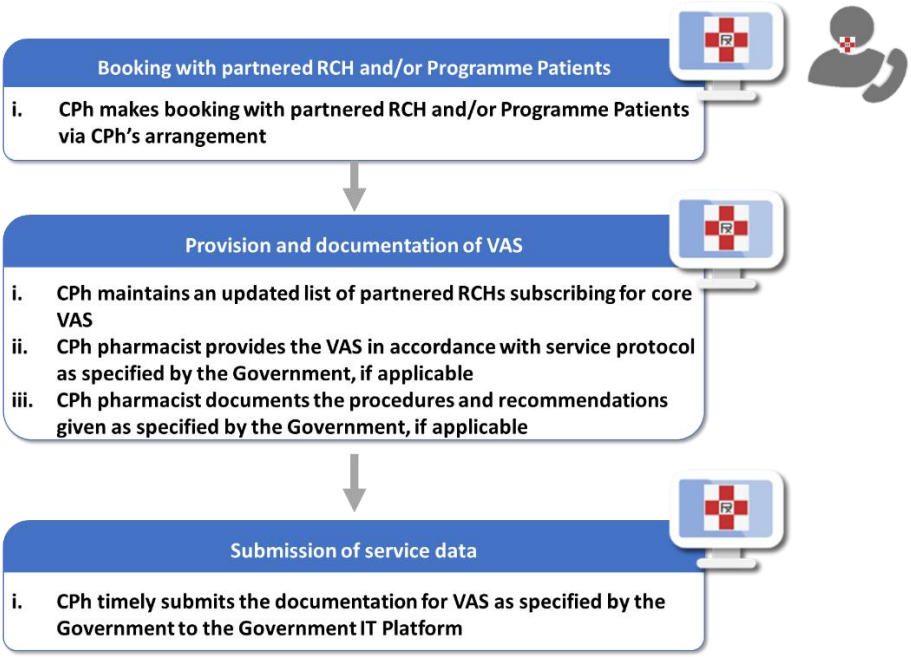
Task to be performed by the CPh manually

The Service workflow is illustrated for reference only and may be updated from time to time by the Government.

III. Monthly collection of patient co-payment and submission of dispensing service fee claim



IV. Provision of Value-added Services to partnered RCH and/or Programme Patients



Appendix 2 – Provisions Relating to eHealth

1. The Contractor shall fulfil and continue to fulfil the following criteria for the duration of the Contract Period:

   i. being a registered healthcare provider ("HCP") for the Hong Kong Government's eHealth;
   ii. establishing and maintaining the necessary infrastructure at its premises where the Contractor will provide the Services, to enable the Contractor and any authorised users appointed by them ("Authorised Users") to access Programme Patients' clinical records through the Government IT Platform and eHealth, and input/upload Programme Patients' information into the Government IT Platform;

   iii. providing a list of the Authorised Users to the Government and informing the Government promptly of any changes to such appointments;
   iv. ensuring all Authorised Users have completed training on the Government IT Platform;
   v. complying with all rules, regulations, codes of practice (COP) and requirements imposed by the Government and eHealth from time to time;
   vi. notifying the Government promptly if the Contractor ceases to be a HCP; and
   vii. complying with its own data retention policy.

2. The Contractor and/or its Authorised Users shall promptly enter such information in relation to a Programme Patient as required by the Government into the Government IT Platform.

3. The Contractor and its Authorised Users shall not print Programme Patient records from the Government IT Platform or use such printed records unless otherwise permitted by the Government and shall not download or take photographs of any Programme Patient records from the Government IT Platform or, unless required or permitted by law, give such Programme Patient records in any form to the Programme Patient, his/her parent or guardian or any person acting for or on behalf of the Programme Patient.

4. The Contractor shall take all necessary steps to ensure that its Authorised Users and employees shall be made aware of and perform the obligations under the Contract applicable to them and shall comply with all rules, regulations and requirements imposed by the Government from time to time. Without prejudice to other rights which the Government may have, the Government is entitled to remove any Authorised User's access to the Government IT Platform in case of non-compliance.

5. All copyright and other intellectual property rights in respect of the compilation of data contained in or entered into the Government IT Platform shall be vested in and belong to the Government. The Contractor and its staff shall not infringe the copyright and other intellectual property rights of the Government and shall indemnify the Government against any loss, damages, liability, cost and expense arising from such infringement.

6. The Contractor and its Authorised Users shall only use the data in the Government IT Platform for the provision of Services and the performance of the Contract (the "**Purposes**") and exercise reasonable care to protect Programme Patients confidentiality at all times. The Government IT Platform and all data contained in or obtained from the Government IT

Platform shall be protected against unauthorised or accidental access, processing or other use. All access to the Government IT Platform shall be made at secure computer terminals with adequate security measures.

7. The Contractor shall not, and shall procure its Authorised Users not to, share their eHealth accounts with or disclose the passwords to any persons.

8. The Contractor shall make all necessary precautions and measures to ensure the Programme Patients' personal data in the Government IT Platform are secured and protected. The Contractor and its Authorised Users shall comply with all obligations under the law in relation to personal data including the Personal Data (Privacy) Ordinance (Cap. 486 of the laws of Hong Kong) (and the data protection principles), and the policies and requirements of the Government (including any applicable hardware, software, security and upgrade requirements) in the handling, access, use, retention and security of the personal data on the Government IT Platform. The personal data shall not be retained longer than is necessary for the Purposes.

9. If the Contractor and/or its Authorised Users know or suspect that the security or confidentiality of the Government IT Platform or any information contained therein is compromised, they must immediately notify the Government and shall cooperate with the Government in taking all reasonable steps to ensure and protect such security or confidentiality.

10. The information contained in the Government IT Platform is not intended to provide any professional advice and should not be relied upon in any other dealings with the Programme Patients, but as a reference or guidance tool only. The Contractor and its Authorised Users acknowledge that when accessing the Government IT Platform, they are solely responsible for undertaking all necessary clinical and other investigations to provide the Service. It is the Contractor's and the Authorised Users' responsibility to interpret the data on the Government IT Platform with professional knowledge and skills, taking into account their knowledge and assessment of the Programme Patients' history and condition.

11. The Government IT Platform may be updated and amended from time to time and at the time of access by the Contractor and/or its Authorised Users, the data on the Government IT Platform is only a computer generated segment (and not the whole) of the Programme Patients' health records in the Government and may not be updated up to the time of access.

12. Data sent over the Internet cannot be guaranteed to be completely secured. The Government will not be responsible for any damages or expense incurred or suffered by the Contractor, the Authorised Users or any person as a result of any delay, loss, diversion, alteration or corruption of any information provided by the Government over the Internet.

13. The Government IT Platform is provided "as is" without warranty or representation of any kind, express or implied being given by the Government as to any aspect of the Government IT Platform or any data held within it.

14. The Government will not be liable to the Contractor or any of its Authorised Users or employees in any manner for any direct, indirect, special or consequential damages arising or claimed to be arising out of the Government IT Platform. The Contractor shall be liable for any errors or omissions in the information it and/or its Authorised Users provide onto the Government IT Platform and for any loss or damages suffered by the Government for any negligence or misuse of the Government IT Platform by the Contractor or its Authorised Users or employees.

15. No provision in this Appendix shall operate to restrict or limit any person's liability for death or personal injury caused by such person's negligence.

16. The right to access to the Government IT Platform granted by the Government to the Contractor and its Authorised Users shall immediately cease upon expiry or termination of the Contract.

Appendix 3 – IT Requirement Specifications

The Contractor shall ensure the Pharmacy System fulfils the functional requirements, the security and network requirements, and the data interface and connectivity requirements according to specifications provided in this **Appendix 3**, and the prevailing Operation Manual and guidelines which will be provided by the Government when available, and may be updated from time to time in order to ensure the smooth day-to-day operational arrangements for provision of safe and reliable Services.

Functional Requirements	1. Retrieval function for retrieving electronic prescriptions and information specified by the Government from the eHealth/Strategic Health Service Operation Platform (SHSOP) 2. Medication dispensing function ensuring medication safety and complying with the requirements specified in the Operational Manual or guidelines provided by the Government, including but not limited to printing of dispensing label which facilitates code scanning administration technology 3. Clinical note documentation function for pharmacist services or Standard VAS and/or Non-standard VAS provided 4. Patient co-payment calculation function facilitated by the eHealth/SHSOP 5. Submission function for timely submitting full dispensing record, clinical documentation, co-payment payable and information specified by the Government to the eHealth/SHSOP 6. Programme Patient list maintenance function for keeping the pairing information under Community Pharmacy Programme up-to-date 7. User account access control maintenance function 8. Back date input function for system breakdown
Security and Network Requirements to connect to eHealth / SHSOP	Depending on design of overall IT architecture supporting the Programme, the intention is for Pharmacy System to interface with SHSOP and obtain / submit all relevant information originated from / shared to other party systems e.g. eHealth, HA systems 1. System Security & Compliance a. Electronic medical record (EMR) or systems interfacing with eHealth-must undergo independent penetration testing b. Conduct security risk assessment and audit (SRAA) and privacy impact assessment (PIA) every two years c. Security compliance checks and endorsement processes will be performed regularly 2. Data Hosting & Access Control a. All EMR/ Interface systems must be hosted in Hong Kong data centres b. Cloud-based EMR systems must enforce multi-factor authentication (MFA) for privileged accounts c. All users must use MFA when accessing the cloud-based EMR system remotely 3. Protection of healthcare recipient (HCR) Data a. All personally identifiable information (PII) must be encrypted irrespective of the storage media (e.g.: database, file or disk storage level) — PII must not be stored in plain (unencrypted) format. b. Secure management of encryption keys must be implemented and documented in accordance with industry best practices. 4. Secure Network Connections

<table>
<tr><td></td><td>a. Connections from healthcare providers (HCP) to the cloud EMR system must use a virtual private network (VPN) or leased line with adequate bandwidth to support data exchange with eHealth
b. EMR/Interface systems require fixed IP addresses or VPN connections
c. Network setup should support automatic failover or backup connectivity options to maintain service availability during outages or disruptions.
d. At least one public fixed IP address is required to facilitate testing during the development phase</td></tr>
<tr><td>Data Interface and Connectivity Requirements</td><td>Tenderers may obtain from the Government the detailed interface requirements/ specifications (e.g. data requirement specification, technical interface specification) in relation to the Government IT Platform as specified by the Government before the Tender Closing Date.

Part A: Requirements for Retrieving Data from eHealth^

❖ The Contractor shall be able to retrieve the following information from eHealth by conforming to the following interface requirements:

1. Developers' Quick Guide (Overview) for Community Pharmacy Programme
- Retrieve electronic prescriptions and information specified by the Government
- Retrieve Programme Patient list
- Facilitate co-payment calculation
- Facilitate user friendly workflow provided by eHealth App
2. Data Requirement Specification for Electronic Health Record (eHR) Prescription Record and Electronic Health Record (eHR) Dispensing Record [S14]

❖ The Contractor shall be required to conduct an annual compliance checking and endorsement process as given below.

i. Requirement A: The Contractor is required to submit the following security assessment checklist on annual basis:
<table><tr><td colspan="2">Security Assessment Checklist Submitted by Healthcare Providers (HCP)</td></tr><tr><td>Part I, II</td><td>Checklist for Connection Mode B</td></tr><tr><td>Part III (mandatory to submit)</td><td>Checklist with Additional Security Requirement for Data Download HCPs</td></tr><tr><td>Part IV (Applicable for HCPs using Cloud EMR)</td><td>Checklist For Cloud EMR</td></tr><tr><td>Part V (Applicable for HCPs using SaaS EMR)</td><td>Checklist For SaaS EMR</td></tr></table></td></tr>
</table>

Note: HCPs with Mode A or B connection with eHealth can skip Parts I, II, IV and V of the Security Assessment Checklist as the respective Security Compliance Process has already been completed.

ii. Requirement B: The Contractor shall employ a third party provider to perform annual network port and web vulnerability scanning for the Pharmacy System connecting to eHealth.

Part B: Requirements for Submitting Data to eHealth^

Dispensing Service:

❖ The Contractor shall be able to capture the following data using the eHealth FHIR application programming interface (API) for processing and submission of dispensing records and drug order records to eHealth through the specified data exchange interface:
- ePrescription Number
- Transaction reference number (if applicable)
- Healthcare Provider ID
- Healthcare Service Location ID
- Programme Patient eHR No.
- Programme Patient English Name
- Programme Patient HKIC No.
- Programme Patient Date of Birth
- Programme Patient Sex
- Complete dispensing record
- Item order number
- Dispensed duration
- Dispensed quantity
- Copayment information
- Operational information

^Subject to the data and interface specifications as provided by HA and/or the Government

❖ The Contractor shall be able to submit data to the eHealth by conforming to the following data interface requirements:
1. Developers' Quick Guide (Overview) for Community Pharmacy Programme
2. eHR Content Standards Guidebook
3. Data Requirement Specification for Electronic Health Record (eHR) Prescription Record and Electronic Health Record (eHR) Dispensing Record [S14]

❖ The Contractor shall be able to submit the records to eHealth by conforming to the following business requirements:

1. Records could be submitted by batch.

	2. One batch of data submission could include more than one dispensing record identified by ePrescription number. 3. If modification of dispensing record is required, all of the previously submitted dispensing records within the same refill transaction have to be submitted together. Standard Value-added Services (VAS): ❖ The Contractor shall submit to eHealth the clinical documentation of Standard VAS provided through the Pharmacy System with specified data exchange interface. The dataset* includes but not limited to: - Mode of service delivery - Allergy, ADR - Medication-related history - Problem(s) identified - Clinical Note (including but not limited to Risks identified, Risk factors, Clinical assessment, Clinical progress) - Intervention(s) - Referral, Communication letter with healthcare professionals *Updates to the data specifications, as defined by the Government, will be provided to Contractor from time to time. ❖ The Contractor shall be able to submit data to the eHealth by conforming to the eHealth standards for the eHR content dataset - eHR Content Standards Guide book

Appendix 4 – The Proof of Readiness of the IT system

(to be submitted within sixteen (16) weeks from the date of Letter of Conditional Acceptance)

Part A: Delivery to the Government and fulfilment of the following IT requirements, at the Contractor's own costs and expenses, to the full satisfaction of the Government. The successful Tenderer shall be required to fulfill the following tasks with respective deadline as specified below.

	Task Description	**Deadline**
1	Confirm IT knowledge checklist as list in Part B below	Within four (4) weeks from the date of Letter of Conditional Acceptance
2	Preparation of hardware/software for connectivity network	
3	Perform end-to-end network connectivity testing *(in collaboration with HA IT&HI Team)*	
4	Provide sample dispensing data and drug order data which is in compliance with the data and interface standards issued by HA and/or the Government for verification as directed by the Government *(in collaboration with HA IT&HI Team)*	
5	Programme development for exchange of prescribing and dispensing record electronically	
6	Perform end-to-end testing in relation to exchange of prescribing and dispensing record and interface testing with eHealth IT systems *(developed by and in collaboration with HA IT&HI Team)*	Within sixteen (16) weeks from the date of Letter of Conditional Acceptance
7	Production rollout of IT connectivity including exchange of prescribing and dispensing record electronically	Within sixteen (16) weeks from the date of Letter of Conditional Acceptance
8	Documentation submission to HA and/or the Government to confirm the successful completion of interface testing	Within sixteen (16) weeks from the date of Letter of Conditional Acceptance

Part B: The successful Tenderer shall confirm it has knowledge according to the checklist below within four (4) weeks from the date of Letter of Conditional Acceptance.

Essential IT Knowledge Checklist for Achieving Sharing of Records with eHealth/SHSOP

Checklist	IT knowledge
	1. Quick Identification 1.1. QR code scanning technology
	2. Connecting Systems for Health Data Sharing 2.1. Procurement, installation, and use of Hong Kong Post e-Cert certificates (Server and Encipherment) 2.2. Secure communication protocols: HTTPS, TLS, and Public Key Infrastructure (PKI)
	3. Data Formatting and Exchange 3.1. FHIR API integration for healthcare data interoperability 3.2. Web service development using RESTful APIs with OAuth authentication 3.3. Data formatting and exchange using JSON and XML
	4. Reliable System Infrastructure 4.1. Stable systems with automatic failover and rapid recovery to minimize service interruptions. 4.2. Continuous health checks and alerts for early issue detection, plus regular updates to keep applications, web, and database servers running smoothly. 4.3. Use of reliable, industry-standard platforms (such as WildFly for applications, Apache for web services, MySQL/Oracle for databases) to ensure secure and efficient operations.