

eHealth+

# eMedication



## IT Security Preparation

30 Sep 2024

Dr Wong Wing Nam

Mr Stephen Wai

Mr German Leung

*Logistics and Supply Chain MultiTech R&D Center (LSCM)*

Mr Ricky Hui

*Hospital Authority, IT&HI*

# eHealth eMedication Connectivity Preparation



15-Aug-2024  
**eMedication Data Connectivity and Technical Briefing Session**

On the 15th August 2024, we have successfully organised a **Data Connectivity and Technical Briefing Session** aims to empower participants with the knowledge and skills necessary to implement the eHealth Medication Data Standards, and obtain medication data through a system interface connected with eHealth. The session has attracted over 90 attendees, covering most RCH IT partners.

Objectives for the session is to facilitate RCH IT vendor/team understanding of the data and technical preparation and pre-requisites for obtaining data from eHealth. Also to facilitate RCH IT and clinical team to interpret the data obtained from eHealth correctly and to identify system changes that may be required in the RCH system to present correctly and use the data obtained from eHealth.

[Download the presentation materials](#)

1. Kick-off Meeting for eMedication 25 Mar 2024
2. Technical and Data Preparation 15 Aug 2024
3. Administrative Preparation 16 Aug 2024
4. IT Security Preparation 30 Sep 2024
5. Data Preparation (Advanced) and iAm Smart Authentication 4 Oct 2024

Step-by-Step Preparation for **eMedication Data Connectivity**  
4 Steps for requesting and preparing for eHR medication data connectivity from eHealth.

- Step 1: Submit Request**  
Download and fill in the **eHealth+ Medication Data Download Request Form** and submit it to LSMC ([emedication@lscm.hk](mailto:emedication@lscm.hk)).
- Step 2: Administrative Preparation**  
Follow the guidance to register eHealth and devise relevant internal guidelines and policies for using data obtained from eHealth.
- Step 3: Technical Preparation**  
Undergo technical and data preparation for Electronic Medical Record System (eMRS) for system interfacing and data connectivity with eHealth.
- Step 4: Testing and Approval**  
Test and certify eMRS as capable of connecting with eHealth.

16-Aug-2024  
**eMedication Administrative Preparation Briefing Session**

On the 16th August 2024, we have organised an **Administrative Preparation Briefing Session** which aims to share with Residential Care Homes the steps-by-steps processes of registering eHealth for their residents and other administrative processes essential for obtaining medication data from eHealth. The session has successfully attracted over 280 RCH representatives and IT partners, yielding a fruitful result.

[Download the presentation materials](#)

<https://emedication.lscm.hk/en/index.html>

# LSCM eMedication Connectivity Platform

## Step-by-Step Preparation for eHR Medication Data Download

- Step 1 **Submit Proposal**
- Step 2 Administrative Preparation
- Step 3 Preparation Procedures
- Step 4 Testing and Approval

### Submit eMedication Data Download Proposal

Please read the following information for completing the request for medication data. Please download the eHR Data Download Proposal Form, fill in the required information, and submit it to [\(emedication@lscm.hk\)](mailto:Hong Kong Logistics and Supply Chain MultiTech R&D Centre (LSCM) (emedication@lscm.hk)).

Residential Care Home (RCH) and IT vendors are advised to seek LSCM's advice and guidance when filling out the proposal form.

[Download eHR Data Download Proposal Form](#)

Data download must be requested by an RCH that has registered eHRSS as a Healthcare Provider and must provide justifications and valid use cases for obtaining data from eHRSS.



#### 1. Purpose of Medication Data Download

Description of the **existing workflow** of medication management in the RCH supported by the RCH IT system and the intended uses of the medication data from eHRSS for the benefits of medication management operation.

Describe the benefits in terms of efficiency and quality improvement in overall medication management.

#### 2. Information Regarding RCH

**Number of residents** in the RCH. For composite submission for multiple RCH using the same RCH system, please provide a list of RCHs and the number of residents in each of the RCH.

Whether the RCH(s) have **registered eHRSS** as an eHR healthcare provider and the percentage of residents registered as eHR healthcare recipients

The **existing medication management practice** in the RCH(s)

#### 3. Information Regarding the RCH IT System

The **technical model** of the RCH IT system, whether cloud or web-based or on-premise local installation.

**List of features** of the RCH system, in general and in particular for medication management

Whether and the **number of RCHs which have adopted third-party medication systems**, e.g. automated packaging, if any

Adoption of any **medication data standard or structure** or reference terminology in the existing system

Description of **IT security measures and functions** that have been adopted.

#### 4. Information Regarding Users of RCH IT System

**Number of healthcare professionals**, including doctors, nurses, pharmacists, dispensers, and healthcare assistants, etc using the medication-related functions

User authentication means adopted (e.g. password, one-time password or others)

Whether there are any security or privacy assessments done in the RCH system in the past 2 years, if any, the date of assessment and the consultancy firm carrying out the assessment.

## Step-by-Step Preparation for eHR Medication Data Download

- Step 1 Submit Proposal
- Step 2 Administrative Preparation
- Step 3 **Preparation Procedures**
- Step 4 Testing and Approval

### Medication Data Standard, System Security and Other Preparation Procedures

The Residential Care Home (RCH) IT system vendor must implement eHRSS Medication Data Standards and fulfil system interfacing specifications to ensure accurate interpretation and use of data downloaded from eHRSS.

The RCH IT system must also achieve the required security standards and implement the procedures for handling data obtained from eHRSS.

The RCH and RCH IT System must devise adequate internal security policies and procedures for handling data obtained from eHRSS to provide approved healthcare purposes. To fulfil the requirements, an independent Security Risk Assessment and Audit (SRAA) should be carried out, and the report should be sent to eHRO.



#### List of documents relevant to...

- Medication Data Standards**
- Security Standards

#### Related Form

##### eHR Dispensing Record

Healthcare provider (HCP) registering with the Electronic Health Record Sharing System (eHealth)



##### eHR Prescribing Record

Providing information of additional HSL (only applicable to HCP with more than one HSL)



##### Healthcare Recipient Index

Healthcare provider (HCP) registering with the Electronic Health Record Sharing System (eHealth)

##### eHR Content Codex

Healthcare provider (HCP) registering with the Electronic Health Record Sharing System (eHealth)

##### Hong Kong Medication Terminology Table

Healthcare provider (HCP) registering with the Electronic Health Record Sharing System (eHealth)



[Previous Step](#)

[Next Step](#)

# Step-by-Step Preparation for Data Downloading

## 1. Request

1. Submit request
2. Submit RCH list

## 2. Administrative Preparation

1. eHR Registration
  - HCP
  - HCR
  - Sharing / Download
2. Privacy Policies and Procedures
  - PIA

## 3. Technical Preparation

1. Data Standards (HKCTT/HKMTT)
2. Interfacing Standards (HL7 FHIR)
3. Security
  - Security Checklist
  - SRAA

## 4. Testing and Approval

1. Data and Integration Tests
2. Formal approval by eHRO

# Agenda

- IT Security Checklist walkthrough
- Security Upgrade Options
- Government funding for secured RCH system solution adoption

# eHR Security Assessment Checklist










eHR Security Assessment Checklist  
for Clinical Data Download  
[G72]  
Version 1.0.1

## IT Security Requirements:

1. General for healthcare providers
2. Large healthcare provider
3. Data download
4. Public Cloud for single HCP
5. Public Cloud for multiple HCPs

# “RCH Management Solution with Secured eHealth Connectivity Capability”

| IT Security Features  | IT System   | RCH   |
|---|---|---|
| <p><b>Hardware and Software Security</b></p> <p>1. Hardware and Software Security: installation of upgraded computer hardware and wireless connection devices, enhancing physical security controls, and updating antivirus, anti-malware software, and security patches.</p>   |   |    |
| <p><b>Adoption of an Electronic Medical Record system (eMR) / RCH Management System with key enhanced security features:</b></p> <p>2. Robust user authentication (including strong password and 2-factor authentication using iAm Smart authentication), access controls, and comprehensive logging for monitoring and audit purposes.</p> |    |   |
| <p>3. Integrated encryption protocols for data at rest and in transit, along with enhanced backup functionalities for data integrity and disaster recovery.</p>   |    |   |
| <p>4. Securing network connections through VPNs, fixed IP internet addresses, IP filtering to ensure the protection of data transmitted between users’ workstations and the eMR system.</p>   |   |   |
| <p>5. Regular Security Risk Assessment and Audit to ensure timely and continuous security risk identification and rectification</p>   |  |   |
| <p><b>Security Policies and Procedures</b></p> <p>6. Development and adoption including user training for relevant policies and procedures for proper use and monitoring of the use of the data in the eMR and handling of personal data</p>  |   |  |

# Hypertext Transfer Protocol Secure (HTTPS)

## Rationale for Using HTTPS:

HTTPS (Hypertext Transfer Protocol Secure) is essential for securing applications in the cloud. It encrypts data transmitted between a user's device and the cloud server, safeguarding sensitive information like login details and personal data from interception, eavesdropping, and man-in-the-middle attacks.

- **Data Encryption:** Utilizes SSL/TLS protocols to make data unreadable to unauthorised interceptors.
- **Authentication:** Verifies server identities to prevent users from connecting to fraudulent sites using certificates recognised by trusted Certificate Authorities.
- **Data Integrity:** Ensures data remains unaltered during transmission, preventing tampering with user inputs or financial information.

## Technical Setup:

- **Certificate Acquisition:** Secure an SSL/TLS certificate from a trusted Certificate Authority. Choose from various levels of validation based on security needs and budget.
- **Configuration:** Install and configure the certificate on your server to enable HTTPS, ensuring all connections are secure.

## Maintenance:

- **Certificate Renewal:** Regularly renew SSL/TLS certificates to maintain security credentials. Automate renewal processes with tools like Let's Encrypt.
- **Security Updates:** Keep server software up-to-date to protect against vulnerabilities in SSL/TLS protocols and encryption methods.

# HTTPS (Hypertext Transfer Protocol Secure)

## Provider and User Consideration:

- **Provider:** Enhancing trust and compliance through visible security measures like HTTPS can significantly boost the provider's reputation and user confidence.
- **User Experience:** With encryption technologies that minimize latency, users could benefit from enhanced security without significant performance drawbacks.

## Step-by-Step Guide for Setting Up HTTPS in an Ordinary Cloud Service

Setting up an HTTPS connection for a web application hosted on Cloud Services involves several key steps to ensure secure communication between your users and the application. Here's a simplified, step-by-step guide based on the typical cloud service setup using Elastic Beanstalk and Application Load Balancers:

### Step-by-Step Guide to Setting Up HTTPS:

1. **Acquire an SSL/TLS Certificate:** Use Cloud Service Certificate Manager to manage and deploy certificates
2. **Configure the Load Balancer:** Set up an Application Load Balancer to handle HTTPS requests, attaching your SSL/TLS certificate.
3. **Set Up Security Groups:** Adjust security settings to allow HTTPS traffic on port 443.
4. **Configure Your Application:** Ensure encryption is extended to the server hosting the application if necessary.
5. **DNS Configuration:** Update DNS records to point to the load balancer.
6. **Test and Validate:** Confirm the setup by accessing the application via HTTPS and checking for security compliance.

# Virtual Private Network (VPN)

## Rationale for Using HTTPS:

A Virtual Private Network (VPN) is critical for securing remote connections to cloud-hosted applications. It creates a secure tunnel between a user's device and the cloud server, encrypting all transmitted data. The VPN aims to prevent unauthorised access and ensure privacy and security for data exchange across potentially insecure internet networks.

- **Data Encryption:** Encrypts all data passing through the VPN, ensuring it remains inaccessible to unauthorised parties.
- **Authentication:** Establishes a secure connection by authenticating the user and the network, preventing unauthorised access.
- **Data Integrity:** Protects data from being altered or intercepted during transmission, ensuring the reliability of the information sent and received.

## Technical Setup:

- **VPN Gateway Creation:** Set up a VPN gateway in the cloud environment to handle incoming VPN connections.
- **Configuration:** Configure VPN client software on users' devices to connect to the VPN gateway. This involves setting up security protocols and encryption methods.

## Maintenance:

- **Monitoring Connections:** Regularly monitor VPN connections for security breaches or unauthorised access.
- **Updating Software:** Keep the VPN client and gateway software up-to-date with the latest security patches and updates.

# Virtual Private Network (VPN)

## Provider and User Consideration:

- **Provider:** Implementing a VPN enhances the service provider's security profile, fostering trust among users and clients.
- **User Experience:** Users benefit from enhanced security. Although VPNs slightly reduce the connection speed due to encryption processing, modern VPNs are designed to minimise this impact.

## Step-by-Step Guide for Setting Up VPN in an Ordinary Cloud Service

Setting up a VPN connection for a web application hosted on Cloud Services involves several vital steps to ensure a VPN connection for a web application hosted on Cloud Services involves several vital steps to secure communication:

Step-by-Step Guide to Setting Up VPN:

1. **Create a Virtual Private Gateway:** Set up a VPN gateway in your cloud service manager to handle incoming VPN connections.
2. **Configure the Customer Gateway:** On the user's side, set up a customer gateway which could be a physical device or software application.
3. **Establish VPN Connections:** Link the virtual private gateway to the customer gateway using VPN service.
4. **Set Up Route Propagation:** Adjust route tables to direct traffic through the VPN connection.
5. **Security Group Configuration:** Modify security groups to allow traffic only from the VPN connection.
6. **Testing and Validation:** Test the VPN connection for integrity and performance to ensure all configurations are correctly set up.

# Fixed IP Address, IP Whitelisting, and Geolocation Filtering

## Rationale for Using Fixed IP Address, IP Whitelisting, and Geolocation Filtering:

**Rationale for Using Combined Security Measures:** Implementing a combined approach of fixed IP address connections, IP whitelisting, and geolocation filtering significantly enhances the security of cloud-hosted applications. This multi-layered strategy ensures that only authorised users from specific locations can access the application, reducing the risk of unauthorised access and potential cyber-attacks.

- **Fixed IP Address Connection:** Ensures that connections to the cloud service are stable and secure, coming from a known, unchanging IP address.
- **IP Whitelisting:** Restricts access to the application to only those IP addresses that are pre-approved, blocking unauthorized IPs.
- **Geolocation Filtering:** Allows or blocks traffic based on geographic locations, adding an extra layer of security by ensuring that users are accessing the application from expected regions.

## Technical Setup:

- **Network Configuration:** Configure the cloud environment to accept connections only from specific, static IP addresses.
- **Implement IP Whitelisting:** Set up access control lists on the application's firewall or within the cloud service settings to allow only whitelisted IP addresses.
- **Geolocation Filtering:** Integrate geolocation filtering tools or services that support blocking or allowing traffic based on geographic location.

## Maintenance:

- **Regularly Update IP Whitelists:** Update the whitelists to include new IPs or remove ones that are no longer needed.
- **Monitor and Adjust Geolocation Settings:** Update the geolocation rules based on threat intelligence and user location data.
- **Security Audits:** Regularly audit the security settings to ensure that the measures are effective.

# Fixed IP Address, IP Whitelisting, and Geolocation Filtering

## Provider and User Consideration:

- **Provider:** This approach demonstrates a high commitment to security, potentially increasing trust among users and clients, particularly those in sensitive industries.
- **User Experience:** While this method enhances security, it may restrict access for users accessing the cloud service outside specified locations.

## Step-by-Step Guide for Setting Up VPN

Setting up a VPN connection for a web application hosted on a cloud service involves several key steps to secure communication:

Step-by-Step Guide to Setting Up VPN:

1. **Configure Fixed IP Addresses:** Set up Elastic IPs to assign static IP addresses to your infrastructure.
2. **Implement IP Whitelisting:** Use security groups and network access control lists to allow traffic only from whitelisted IP addresses.
3. **Set Up Geolocation Filtering:** Integrate with your applications and define geolocation rules that align with your security policies.
4. **Security Group and Network ACL Configuration:** Adjust security groups and ACLs to enforce the policies set by IP whitelisting and geolocation filtering.
5. **Testing and Validation:** Test the configuration thoroughly to ensure that only authorised accesses are allowed and that all filters work as expected.

# Comparison of HTTPS, VPN and IP Filtering/Whitelisting

|                     | HTTPS                                     | VPN   | Fixed IP +<br>Filtering/Whitelisting                                    |
|---------------------|---|---|---|
| Protection Level    | High on data in transit                   | High on data in transit   | High on data in transit   |
| Set up cost         | Low                                       | Moderate<br>Open VPN vs Cloud VPN                                 | Moderate and required<br>subscription of fixed IP<br>communication line |
| Subscription cost   | Low to free                               | Moderate to high<br>(Cloud VPN)                                   | Moderate  |
| Set up effort       | Set up features of most<br>cloud solution | Manual set up of VPN<br>gateway and connections<br>and VPN Client | Manual configuration of<br>network rules and<br>whitelisting policies   |
| Maintenance effort  | Renewal of certificates                   | Server and Client-side<br>configuration                           | Filtering and whitelisting<br>criteria                                  |
| End user experience | Seamless                                  | Good. Could support<br>remote access                              | Seamless with minimal<br>latency  |
| Scalability         | High                                      | Medium  | Medium  |

# Setting up a (“Strong”) Password could be Frustrating



NN/g

Training & UX Certification ▾

Articles & Videos

Consulting

Reports & Books


About NN/g ▾

## Password Creation: 3 Ways To Make It Easier



Katie Sherwin

April 26, 2015

 Share

**Summary:** By making password requirements visible upfront, allowing users to unmask the password, and showing a strength meter, designers can improve the frustrating user experience of creating a password.

For most people, the experience of creating a password is almost exactly the same as it was 20 years ago. Consider for a moment just how *exceptional* that is, given how much technology has changed in that time. Picture a cell phone from 1995; remember its weight, antenna and tiny dark display. Now picture current smartphones, with large touchscreens, HD cameras, and cloud connectivity for infinite storage. It's quite a different experience. And yet, [coming up with and remembering compliant passwords is as difficult as it was in 1995](#). (Password managers, which generate random strings of characters and store them on the users' behalf, and biometric identifiers such as TouchID are standout exceptions to an otherwise stagnant arena of user-authentication technology.)

<https://www.nngroup.com/articles/password-creation/>



Logistics and Supply Chain MultiTech R&D Centre  
物流及供應鏈多元技術研發中心

# 1. Show the Rules

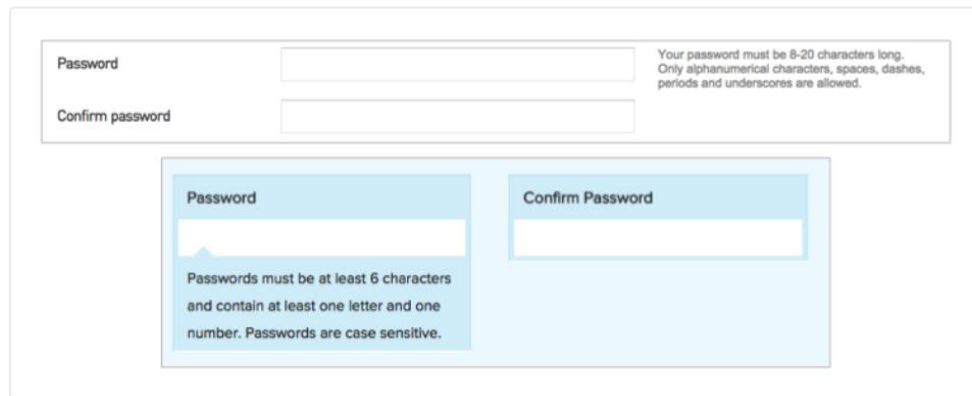
**State the password requirements and ensure that the user can see them the entire time the field before and when it is selected**

**- i.e. Password requirements should be visible when the user is creating the password**

Don't hide the rules and complain to the users when they are not successful

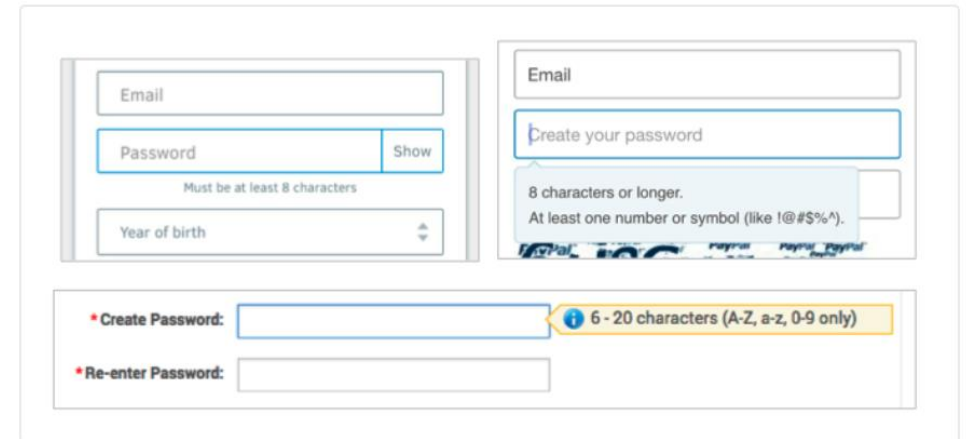
Don't put the rules on a link/tooltip (most people won't notice it or won't bother expanding that link)

Don't put the rules in the placeholders in the input field (the information will disappear exactly when it is most needed)



The screenshot shows a form with two input fields: "Password" and "Confirm password". To the right of the "Password" field, the requirements are listed: "Your password must be 8-20 characters long. Only alphanumeric characters, spaces, dashes, periods and underscores are allowed." Below the form, a blue callout box highlights the requirements: "Passwords must be at least 6 characters and contain at least one letter and one number. Passwords are case sensitive."

*In these examples, password requirements are visible by default. The designs will vary depending on your site's requirements, but each of these examples successfully conveys the restrictions to the user in advance of their typing: TrueBlue.JetBlue.com (top), ppelectric.com (bottom).*



The screenshot shows a form with three input fields: "Email", "Password", and "Year of birth". The "Password" field has a "Show" button. Below the "Password" field, the requirements are listed: "Must be at least 8 characters". To the right, a blue callout box highlights the requirements: "8 characters or longer. At least one number or symbol (like !@#\$%^)". Below the form, a yellow callout box highlights the requirements: "6 - 20 characters (A-Z, a-z, 0-9 only)".

*These password requirements are revealed when the user activates the password field, either by tabbing, clicking, or tapping: Firefox.com (top left), PayPal.com (top right), Alibaba.com (bottom).*

## 2. Show the Input

[Allow users to unmask the password.](#) Seeing the password will support memory and will allow users to check their work. Show password and let users toggle the visibility with a Hide password control.

Hiding a password increases the cognitive load, increasing error and reducing chance of successful password creation

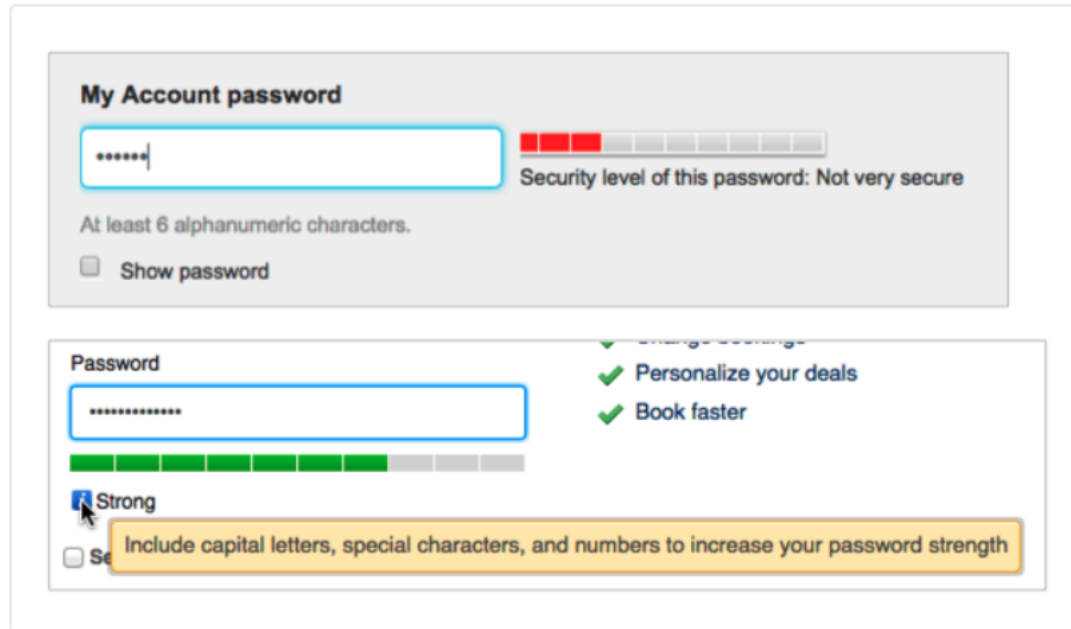
The image displays two examples of password input controls. The top example shows two side-by-side forms. The left form is titled 'My Account password' and has a password field containing ten dots. Below the field is the text 'At least 6 alphanumeric characters.' and a checkbox labeled 'Show password' which is currently unchecked. The right form is also titled 'My Account password' and has a password field containing the text 'hectorthecat'. Below the field is the text 'At least 6 alphanumeric characters.' and a checkbox labeled 'Show password' which is currently checked. The bottom example shows two horizontal password input fields. The top field contains ten dots and has a 'Show password' button to its right. The bottom field contains the text 'Hectorthecat1!' and has a 'Hide password' button to its right. Both bottom fields have a green progress bar at the bottom of the input area.

*These examples allow users to unmask the password: Lan.com (top), Yahoo.com (bottom).*

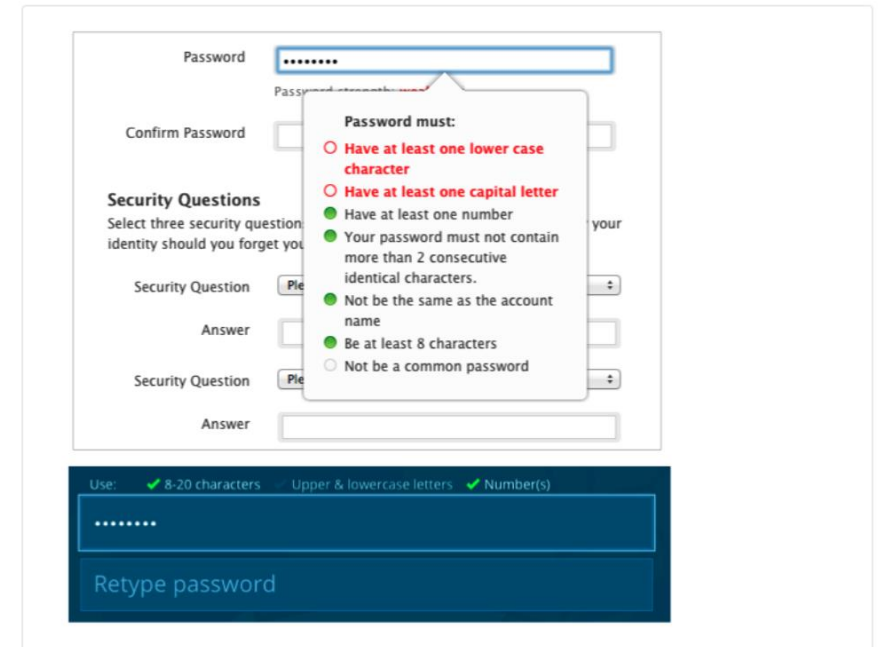
# 3. Show the Strength Meters

Motivate people to create better passwords by showing how secure the password is and whether all requirements are fulfilled

It gives a visual feedback to the progress of fulfilling the password requirements while it is being invented



Strength meters encourage users to create stronger passwords: Lan.com (top), Booking.com (bottom).



These password requirements indicate progress towards meeting all the criteria: AppleID.Apple.com (top), Healthcare.gov (bottom).

# Example of Password Requirement Plugin

## jQuery Password Requirements Plugin Example

The `plugin` displays under your password field a hint popup containing Password Requirements enforced by the security policy of your web app.

.....|

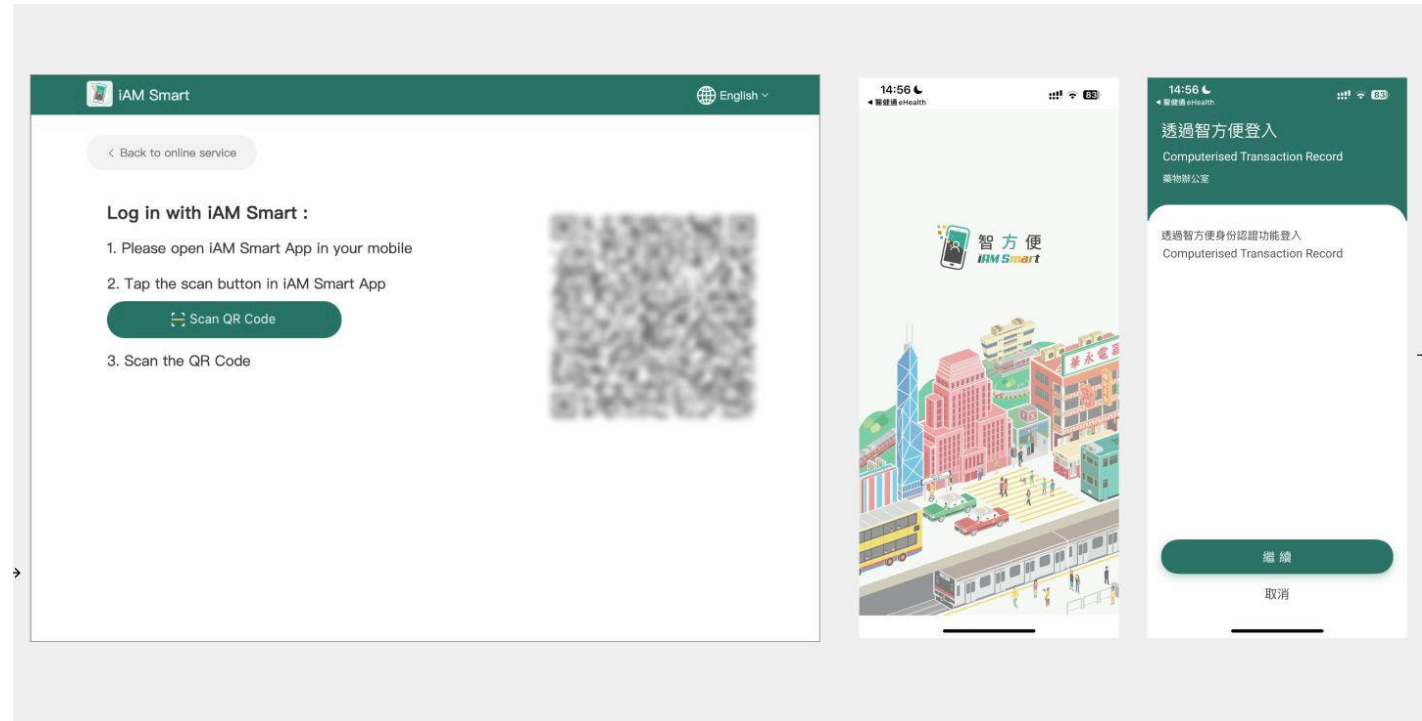
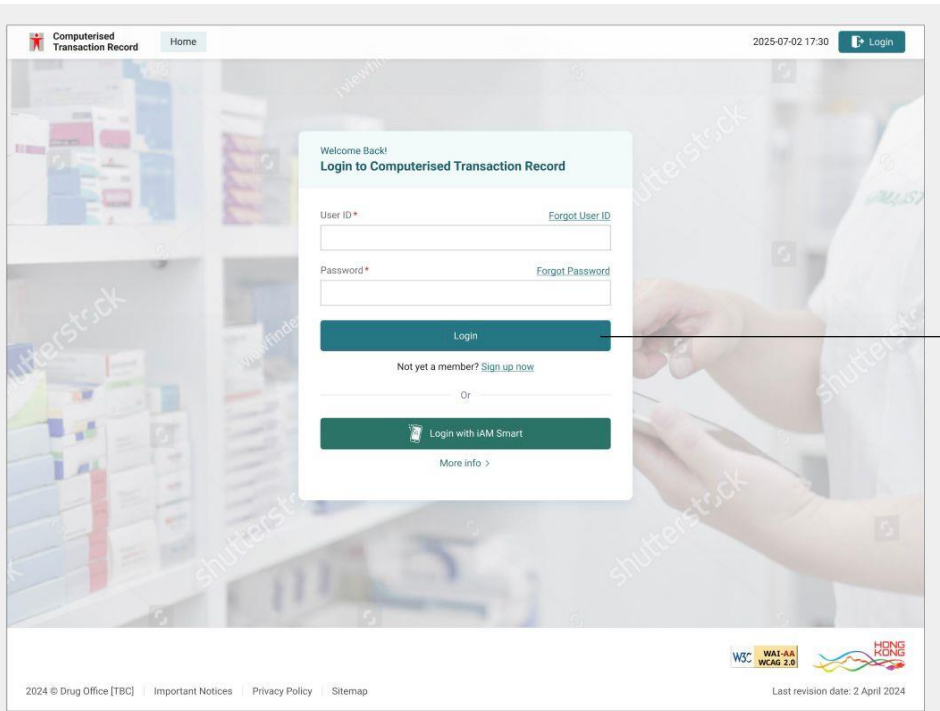
The minimum password length is 8 characters and must contain at least 1 lowercase letter, 1 capital letter 1 number and 1 special character.

- # of characters
- Lowercase letter
- Capital letter
- Number
- Special character

× Premium Application softwar...

[https://www.jqueryscript.net/demo/validate-password-requirements/?](https://www.jqueryscript.net/demo/validate-password-requirements/)

# 2 Factor Authentication with iAM Smart



iAM Smart Authentication Briefing – 4 Oct 2024 (OGCIO)

# Technology Voucher Programme (TVP)

中華人民共和國香港特別行政區政府  
創新科技署  
創新及科技基金

ITCFAS

最新消息 資助計劃 撥款數字 項目檢索 刊物

資助計劃

科技券

### 目標

「科技券」於2016年11月推出，旨在支援本地企業/機構使用科技服務和方案，以提高生產力或將業務流程升級轉型。

### 申請資格

申請科技券資助的本地企業 / 機構，必須符合以下要求 –

- (a)(i) 根據《商業登記條例》(第310章) 在香港登記；或
- (a)(ii) 根據《公司條例》(第622章) 在香港註冊成立的公司；或
- (a)(iii) 根據有關條例在香港成立的法定機構；

及

- (b) 並非本港上市公司，亦並非政府資助機構<sup>2</sup>或任何政府資助機構<sup>3</sup>的附屬公司；

及

- (c) 及在提交申請時在本港有實質業務運作，而該業務須與申請項目相關。

### 計劃特點

- 以3 (政府) :1 (企業 / 機構) 配對模式為項目提供資助。
- 每家企業 / 機構累計資助上限：60萬港元。
- 每家企業 / 機構最多可獲批6個項目。

### 申請

「科技券」全年接受申請。企業 / 機構應先透過科技券計劃管理系統登記為用戶，然後透過系統提交申請書。申請者如在上述系統提交申請時遇到困難而需要協助，可聯絡創新科技署。提交前請先閱讀下列文件。

- 簡介單張
- 科技券簡報
- 申請指南
- 申請66項心在博覽

需要資助建議?

<https://www.itf.gov.hk/l-tc/TVP.asp>

創新科技署  
Innovation and Technology Commission

English

主頁 登記 忘記密碼 活動

# 科技券

登入 登記

登入名稱

密碼 登入

忘記密碼 忘記登入名稱

資助通

由2021年6月8日起，創新科技署委託香港生產力促進局（生產力局）擔任「科技券」計劃的秘書處。如有查詢，請聯絡「科技券」秘書處（電話：2789 7000；電郵：tvp-enquiry@hkpc.org）。

申請人可以從科技券招標系統獲得報價(<https://tvp-eproq.hkpc.org>)

如何使用科技券招標系統

請按此瀏覽生產力局網站

最新簡介會

需要資助建議?

<https://tvp.itf.gov.hk/zh-HK/Home/Index>

# Innovation and Technology Fund



關於我們

最新消息

公共服務

電子服務

服務台

非政府機構資料  
室





聯絡我們

主頁 > 公共服務 > 康復服務 > 特定基金 / 特殊需要信託 / 經濟援助 > 樂齡及康復創科應用基金

## 樂齡及康復創科應用基金

### 最新消息

1. 基金於2024年3月28日至2024年7月31日(下午5時)接受第十批次申請。
2. 第九批次申請結果 (2023年5月至2023年8月)

| 項目 / 名稱 | 檔案下載   |
|---------|--|
| 首輪獲批項目  |  <a href="#">PDF版</a>  |
| 次輪獲批項目  |  <a href="#">PDF版</a>  |

3. 第八批次申請結果 (2022年9月至2022年11月)

| 項目 / 名稱 | 檔案下載   |
|---------|--|
| 第四輪獲批項目 |  <a href="#">PDF版</a>  |

<https://www.swd.gov.hk/tc/aboutus/>

[https://www.swd.gov.hk/tc/pubsvc/rehab/cat\\_fundtrustfinaid/itfund/](https://www.swd.gov.hk/tc/pubsvc/rehab/cat_fundtrustfinaid/itfund/)

# Steps Towards Successful Data Download Pilot



1. Submit [application](#) for data download
2. Submit the [RCH lists](#) using your system
3. Select pilot RCH(s) for preparation
4. Prepare your system for data download UAT
5. Prepare your system for SRAA
6. Work with your RCH clients for PIA

Next Briefing Session:

Data Preparation (Advanced) and iAm Smart Authentication 4 Oct 2024 10:00 to 12:00 noon