eHealth+

eMedication

IT Security Preparation

30 Sep 2024

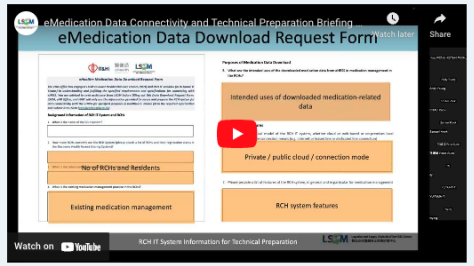
Dr Wong Wing Nam
Mr Stephen Wai
Mr German Leung
Logistics and Supply Chain MultiTech R&D Center (LSCM)

Mr Ricky Hui
Hospital Authority, IT&HI

eHealth eMedication Connectivity Preparation

15-Aug-2024

eMedication Data Connectivity and Technical Briefing Session

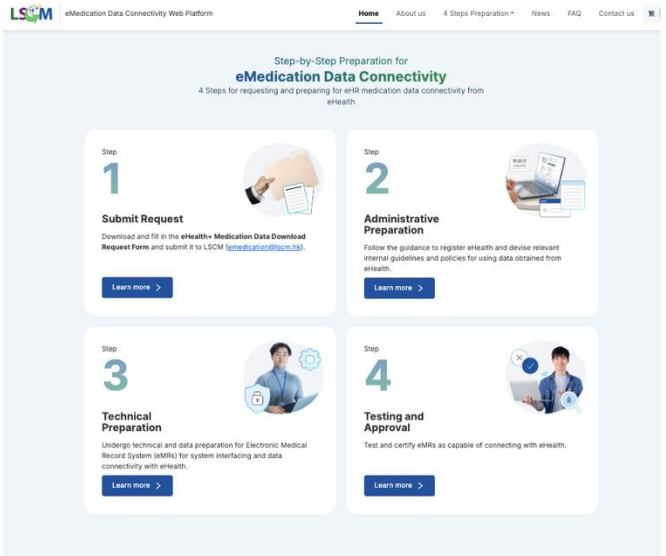


On the 15th August 2024, we have successfully organised a **Data Connectivity and Technical Briefing Session** aims to empower participants with the knowledge and skills necessary to implement the eHealth Medication Data Standards, and obtain medication data through a system interface connected with 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-requisite 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



16-Aug-2024

eMedication Administrative Preparation Briefing Session

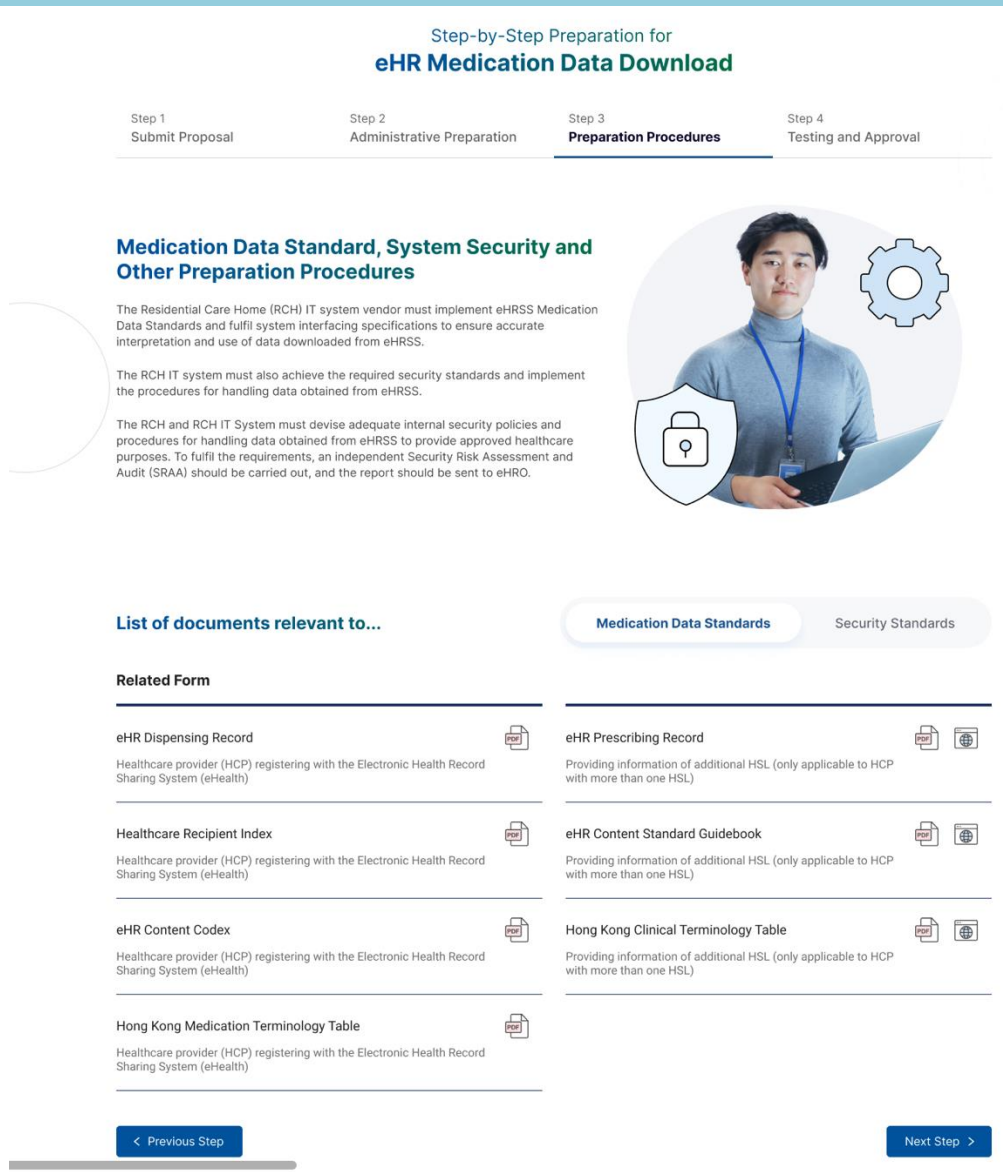
On the 16th August 2024, we have organised an **Administrative Preparation Briefing Session** which aims to share with Residential Care Homes the steps-by-steps processes of registering eHealth for their residents and other administrative processes essential for obtaining medication data from eHealth.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

Download the presentation materials

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

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

LSCM eMedication Connectivity Platform



Portal for all relevant forms, requirements and specifications and links to eHealth.gov.hk

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

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 Polices 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

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
Hardware and Software Security 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.		✓
Adoption of an Electronic Medical Record system (eMR) / RCH Management System with key enhanced security features: 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.	✓	
3. Integrated encryption protocols for data at rest and in transit, along with enhanced backup functionalities for data integrity and disaster recovery.	✓	
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.	✓	✓
5. Regular Security Risk Assessment and Audit to ensure timely and continuous security risk identification and rectification	✓	
Security Policies and Procedures 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		✓

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

Setting up a ("Strong") Password could be Frustrating

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.

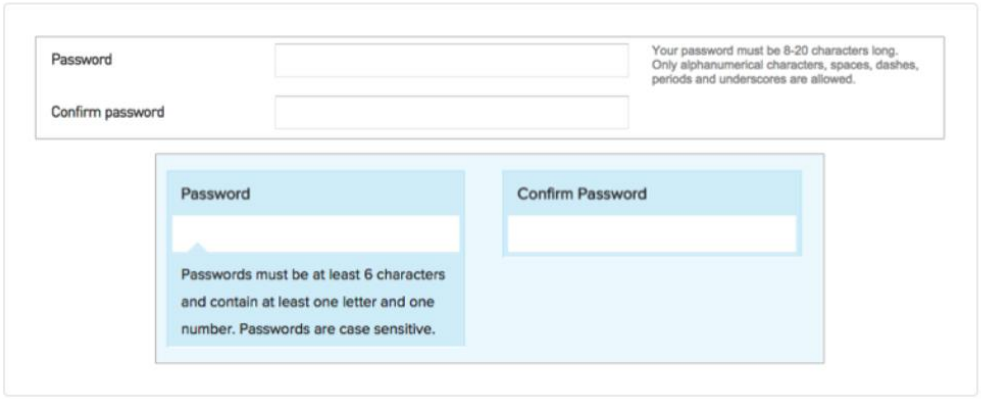
For most people, the experience of creating a password is almost exactly the same as it was 20 years ago. Consider for a moment just how *exceptional* that is, given how much technology has changed in that time. Picture a cell phone from 1995; remember its weight, antenna and tiny dark display. Now picture 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/

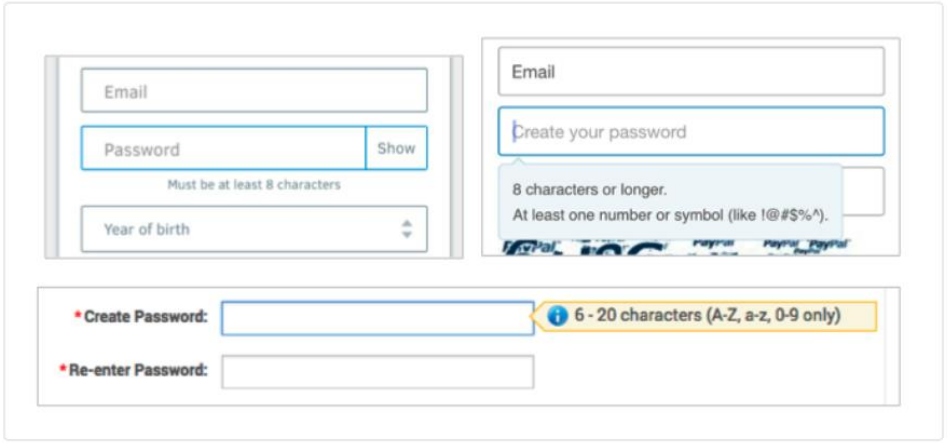
1. Show the Rules

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)



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), pplelectric.com (bottom).

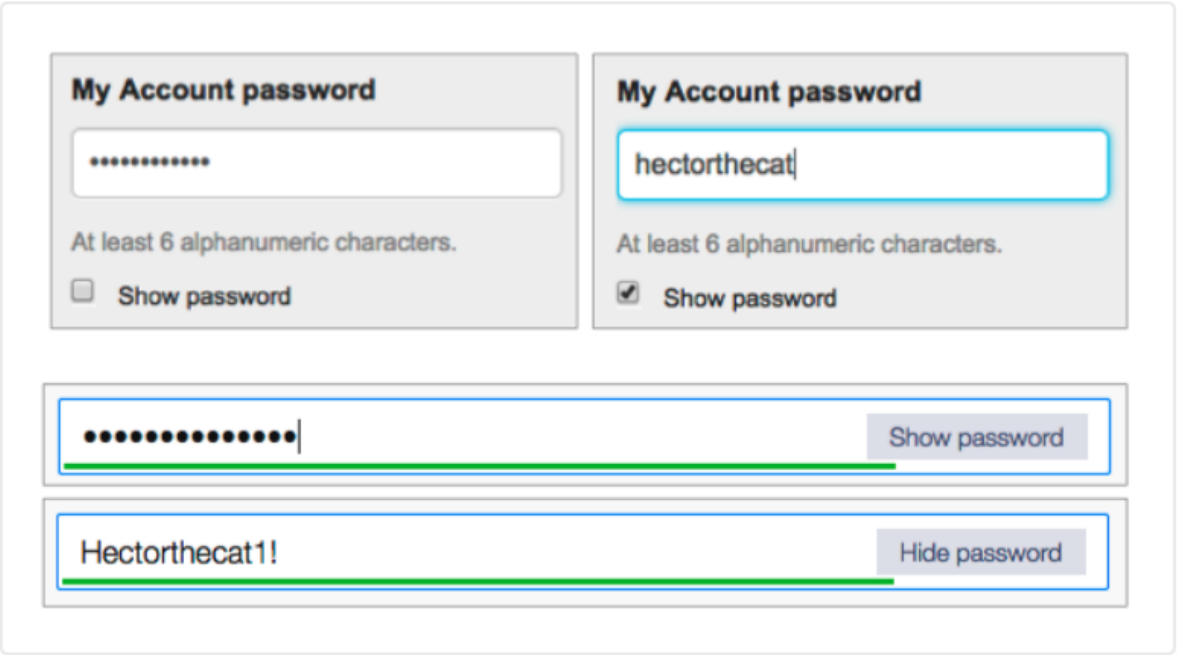


These password requirements are revealed when the user activates the password field, either by tabbing, clicking, or tapping: Firefox.com (top left), PayPal.com (top right), Alibaba.com (bottom).

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

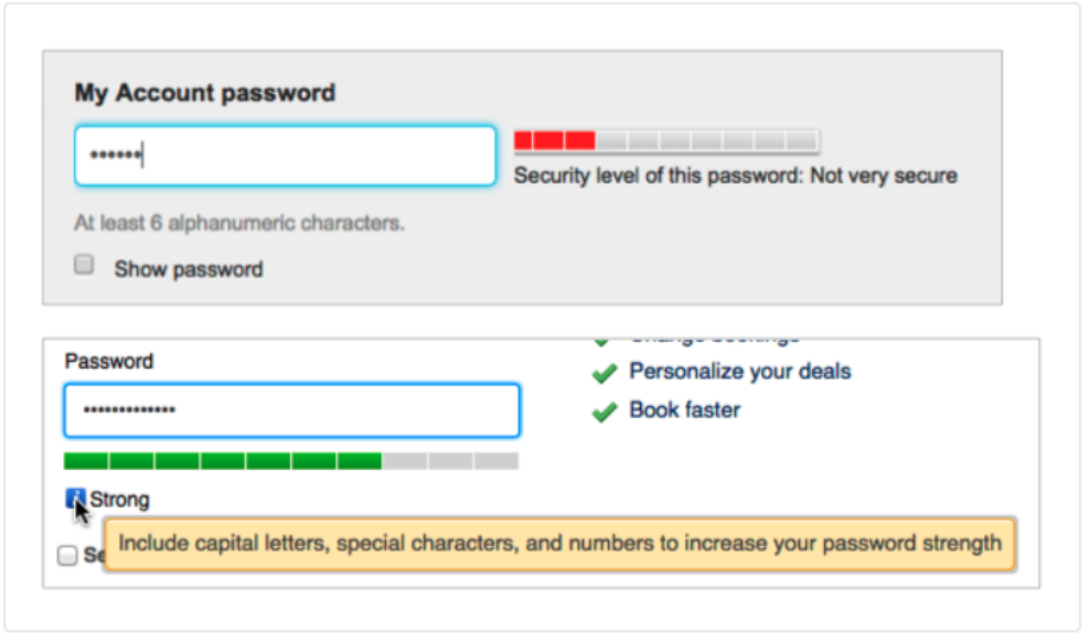


These examples allow users to unmask the password: Lan.com (top), Yahoo.com (bottom).

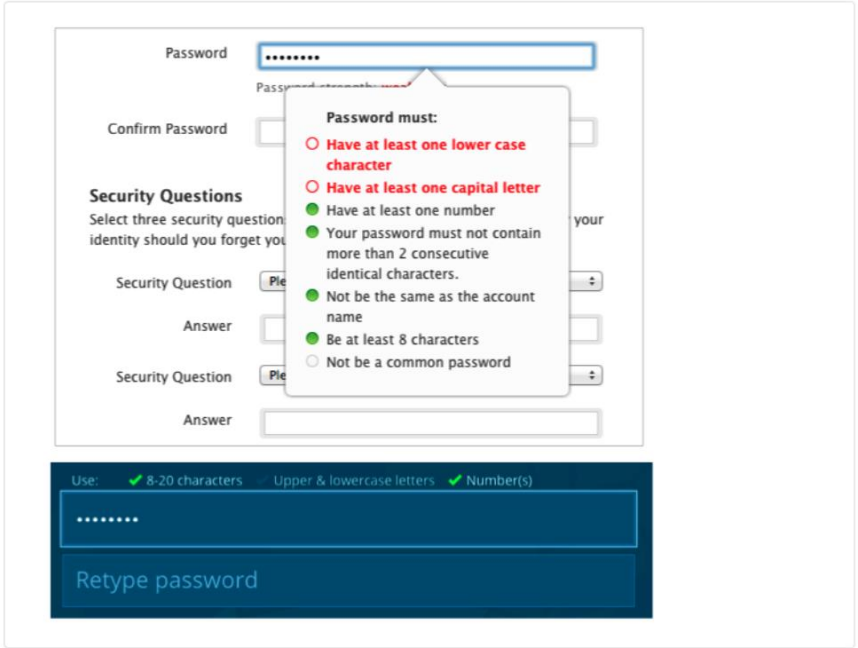
3. Show the Strength Meters

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

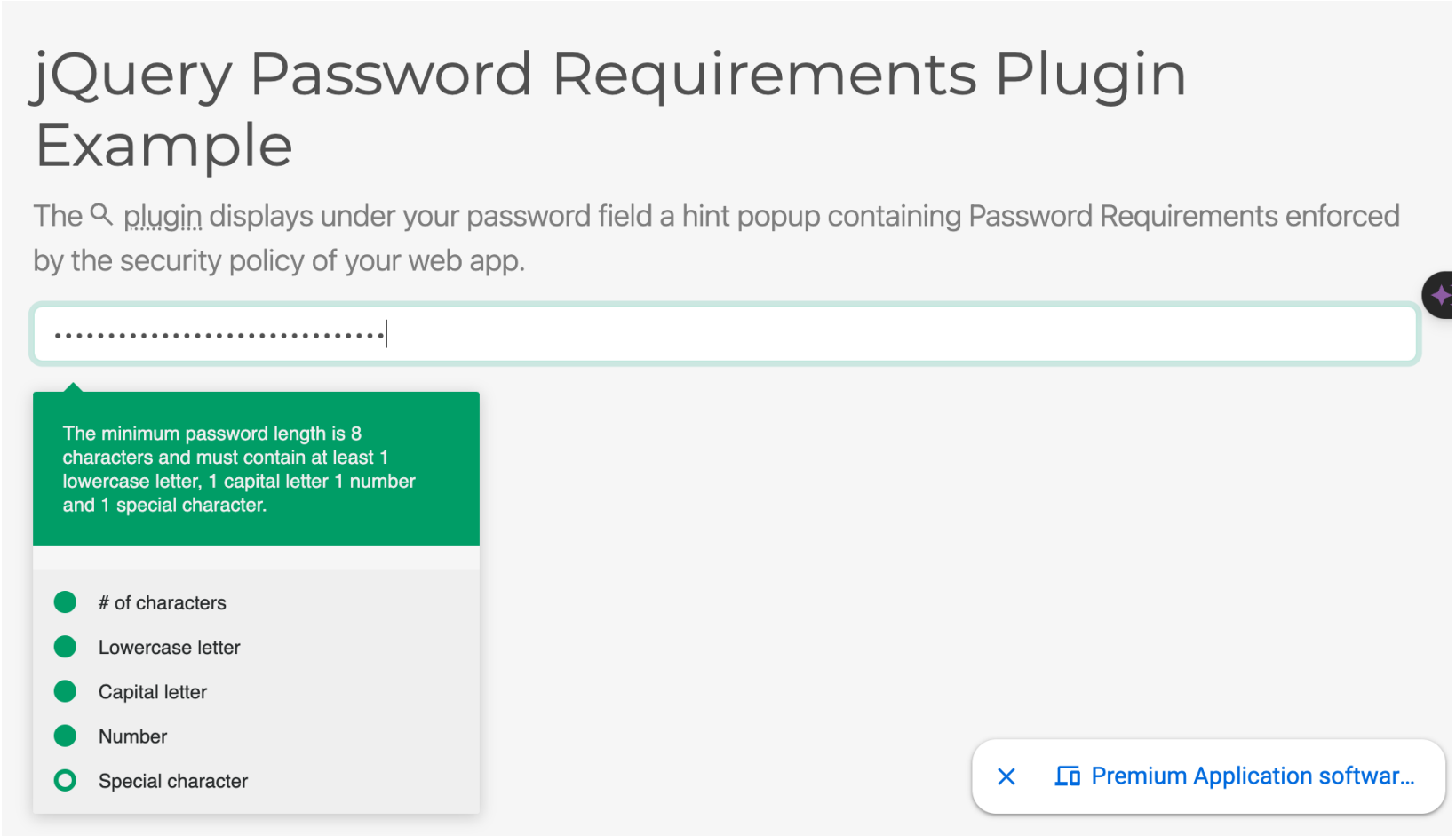


Strength meters encourage users to create stronger passwords: Lan.com (top), Booking.com (bottom).



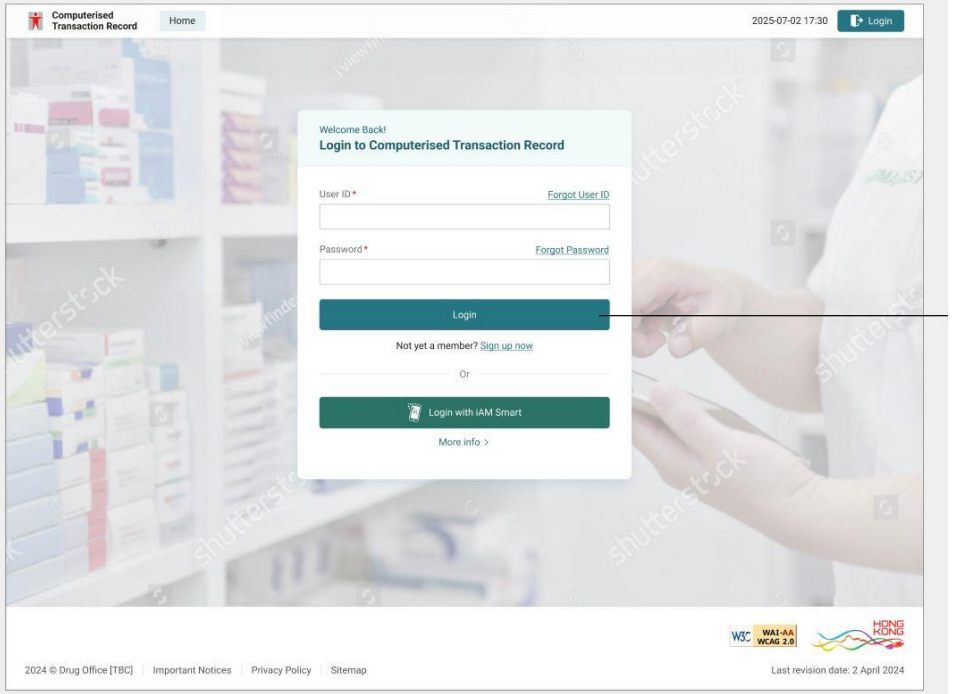
These password requirements indicate progress towards meeting all the criteria: AppleID.Apple.com (top), Healthcare.gov (bottom).

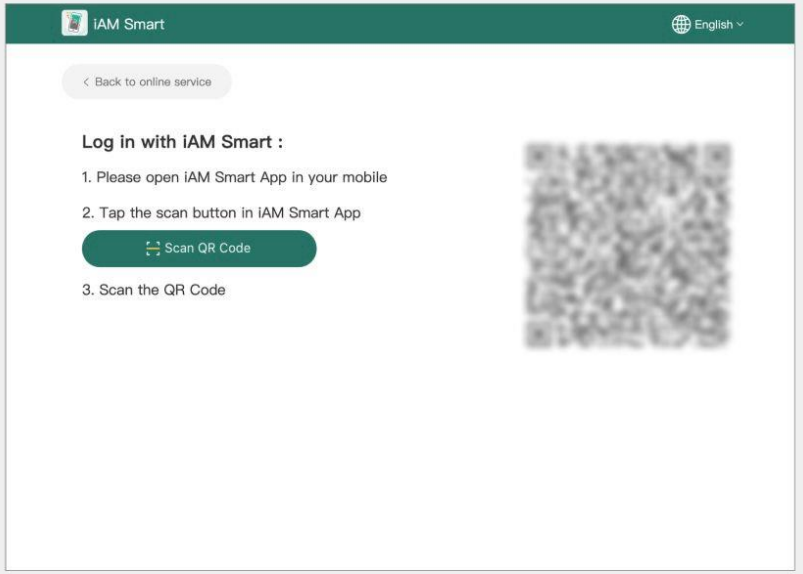
Example of Password Requirment Plugin



https://www.jqueryscript.net/demo/validate-password-requirements/?

2 Factor Authentication with iAM Smart





智方便 iAM Smart

iAM Smart Authentication Briefing – 4 Oct 2024 (OGCIO)

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

Technology Voucher Programme (TVP)

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

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

Innovation and Technology Fund

中華人民共和國香港特別行政區政府
社會福利署

字體大小 | 社署熱線服務

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	PDF版
次輪獲批項目	PDF版

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	PDF版

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

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