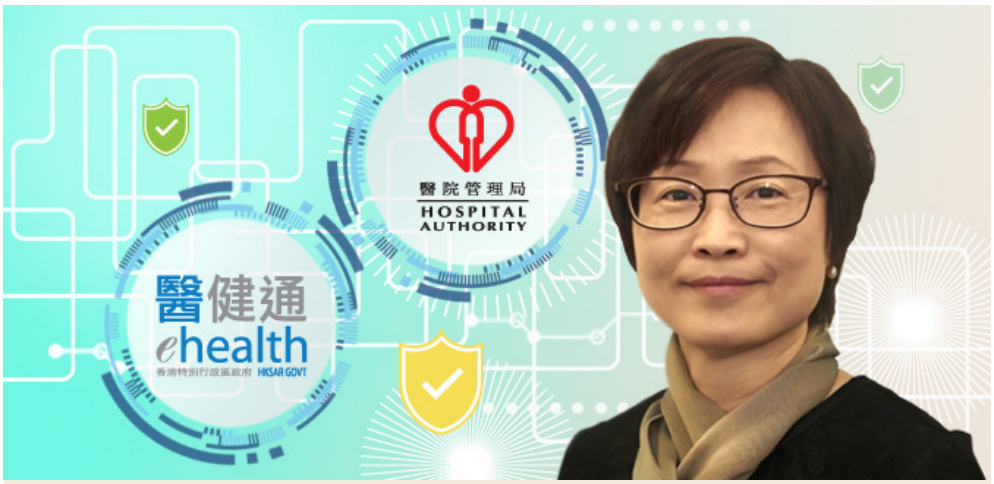
醫健通 ehealth 訊 news ISSUE 19 NOV 2019

Keeping eHRSS and Your Electronic Medical Records Safe from Cyber Security Threats



"Reliable security control is the key to a worry-free experience for users when utilising an information technology (IT) system. In the Electronic Health Record Sharing System (eHRSS), various security measures are implemented at different levels to provide a protected environment for sharing patients' information."

Ms Clara Cheung,
Chief Systems Manager
(IT and Electronic Health Record Operations),
Hospital Authority

Ms Cheung said cyber security requirements for eHRSS are stringent, as a huge volume of sensitive patient data and multiple stakeholders and users are involved. "Patients will be hesitant to join eHRSS if they don't feel secure about their data privacy, despite the many benefits of electronic health record (eHR) sharing," she stressed.

Cyber security requirements for eHRSS are stringent, as a huge volume of sensitive patient data and multiple stakeholders and users are involved

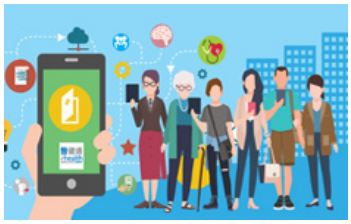
Ms Cheung, who has been leading eHRSS' technical development, said security features have been built into each part of the system management process of eHRSS to guard against fast-evolving security threats such as cyber attacks, and minimise the risk of data breach.

Security-by-Design

Security-by-design is a very important approach in the development of eHRSS to protect patient data and prevent cyber attacks, under which central security controls are included in the system architecture as early as in the design stage, according to Ms Cheung.

"Adding security elements afterwards will be difficult and ineffective," commented Ms Cheung, saying that security-by-design has been widely promoted in the IT industry.

Cyber Security in Healthcare
Mitigating cyber security risks in the healthcare sector



Building and Experiencing the User-Centric Patient Portal
Patient Portal design and usability review

eHRSS for District Health Centres
A key enabler for DHC service delivery

Guides on Proper and Secure Use of eHRSS
Publicity and education on eHRSS account security

eHRSS Updates
Latest publicity and engagement activities

Early from system design, implementation of security controls across the application, system and network levels has been planned to build up a multi-layered defence mechanism

Ms Cheung elaborated, “Early from system design, we have planned to implement security controls across the application, system and network levels in order to build up a multi-layered defence mechanism.

Our security considerations have covered a wide spectrum of scenarios, ranging from typical usages to high-impact security incidents. We have to make sure there are adequate safeguards, and we never assume every eHRSS user is equally conversant about cyber security protection.”

“Such mechanism enables us not only to defend, but also to detect probable cyber attacks so that we can respond quickly to eradicate incident.”

Citing a simple example, Ms Cheung said, “Multiple log-in attempts within a short period of time may imply an attack is going on. Our defence system can spot them out and alert us early for taking security incident response actions.”

Security Principles and Safeguards

Apart from architectural design, eHRSS has also incorporated important security principles and mechanisms to protect data privacy.

According to Ms Cheung, first and foremost, healthcare providers (HCPs) are required to obtain sharing consents from patients for accessing and uploading their eHRs. All data accesses by healthcare professionals (HCProfs) have to be based on the “Patient-under-care” and “Need-to-know” principles.

HCPs are required to obtain sharing consents from patients for accessing and uploading their eHRs

“The role-based access control is another important privacy protection mechanism,” Ms Cheung pointed out, “With pre-defined access rights set in accordance with different HCProfs’ roles in providing clinical care, there are different levels of access to the eHRs in the system.”

Access to eHRSS is secured by two-factor authentication

“In addition, access to eHRSS is secured by two-factor authentication,” Ms Cheung emphasised, “Authorised HCProfs have to provide their unique passwords and the random one-time passcodes generated by their own security tokens to authenticate identity for login to the system.”

“We strive to safeguard data privacy and system security in eHRSS. All accesses will be logged and are subject to audit and inspection. Patients will receive notifications via their selected communication means, i.e. SMS, email or post when their eHRs are accessed. They can report any suspicious access or irregularity immediately once identified,” she continued.

Fun Quiz

Chance to win a prize

Ms Cheung highlighted, “For eHRSS users, the basic but utmost important cyber security measures they can take are to keep their user names, passwords and security tokens safe, and never share their own accounts with others. Since HCProfs’ accounts in eHRSS are assigned to individuals, the HCProfs can use the same account at all HCPs they are authorised to login to eHRSS. In other words, they do not need to remember different user names, passwords and use different tokens with different HCPs. They must not leave their account passwords and tokens with any organisation even when they leave employment with an HCP.”

Patients will receive notifications via their selected communication means, i.e. SMS, email or post when their eHRs are accessed

Future Challenges in Cyber Security for Stage Two Development

Regarding the Stage Two Development of eHRSS, Ms Cheung anticipated that there would be more challenges on data privacy and security protection. “Unlike Stage One when eHRSS users are mainly HCPs, Stage Two eHRSS will involve members of the public accessing their eHRs through the Patient Portal,” she remarked.

“While mobile technology allows users’ convenient access to the Patient Portal, the security risks will be greater at the same time,” she said, referring to the Patient Portal mobile application.

“More security controls will be adopted to minimise the security risks, such as verifying user’s identity with one-time passcode when he/ she logs into the system, restricting the download of sensitive data, etc. We also plan to enable identity authentication through the ‘eID’ launched by the Government with a view to strengthening the portal’s capability in security protection,” Ms Cheung mentioned.

More challenges on data privacy and security protection for Stage Two Development of eHRSS are anticipated as it will involve members of the public accessing their eHRs through the Patient Portal

She added that the security controls will be complemented by industry security standards for mobile devices. “For instance, existing built-in security features of mobile devices like ‘Touch ID’ and ‘Face ID’ are useful complements because they are proven and can be upgraded as technology advances,” she added.

Maintaining High Standard for Security Management

In 2018, eHRSS was awarded the ISO/IEC 27001:2013 certification after its Information Security Management System passed the relevant certification audit. Talking about the key factors for maintaining a high security standard, Ms Cheung said there are three critical aspects - on-going education, regular review and continuous improvement.

Training sessions and seminars are organised to provide up-to-date and latest cyber security information to HCPs, IT colleagues and frontline staff

“Security measures cannot work effectively without users’ cooperation and compliance. Therefore, enhancing the awareness and vigilance amongst HCPs as well as our IT colleagues and frontline staff is also one of our tasks to safeguard data privacy and security of eHRSS. To this end, we have been organising training sessions and seminars to provide up-to-date and latest cyber security information. Regular technical audits, meetings and drills, etc. are also conducted on an on-going basis to evaluate the effectiveness of the existing system security measures and look for areas of improvement,” she remarked.

“Despite all the challenges ahead, we will endeavour to upkeep a high standard of information security management system for eHRSS through continuous improvement by learning from local and international experiences,” Ms Cheung concluded.

Cyber Security in Healthcare

"Healthcare organisations require a holistic approach in managing cyber security risks, integrating information technology (IT), business workflow, data management processes, user access control management and disaster recovery."

Mr Edmond Lai,
Chief Digital Officer,
Hong Kong Productivity Council (HKPC)

Protecting patients' eHRs against different threats has become an important topic for HCPs

The healthcare sector has been facing increasing cyber attacks over the past few years. Protecting patients' electronic health records (eHRs) against different threats has become an important topic for healthcare providers (HCPs). In view of the high sensitivity of patient data, Mr Lai remarked that HCPs have the obligation to implement adequate safeguards and controls to enhance the privacy and security of every datum collected and uploaded.

"Hackers always try every possible way to attack a computer system," said Mr Lai, "These attacks will put data privacy, business operations and service delivery at risk."

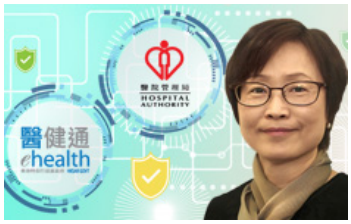
Cyber Security Challenges in Healthcare

Many common cyber attacks in the healthcare sector can be damaging to patient privacy. They also seriously affect the business and data that HCPs are responsible for protecting. Mr Lai said phishing emails and ransomware are two common types of cyber attacks to the healthcare sector.

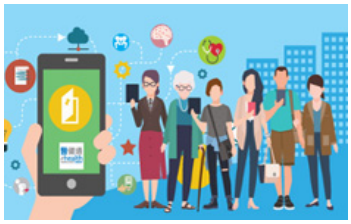
"Ransomware denies users' access to data by encrypting the data stored in systems until a ransom is paid, while phishing email attacks are attempts to steal sensitive information such as user credentials to commit crimes or access an organisation's network for fraudulent activities and gain financial benefits," he explained.

With reference to lessons learnt from cyber security incidents in the healthcare sector overseas, Mr Lai pointed out that there was also rising concern about insider threats. Disgruntled employees, negligent staff and vendors, insecure network and obsolete software, etc. can pose as much risk as cyber criminals.

Ransomware and phishing emails are two common types of cyber attacks. Another threat evolving in healthcare cyber security is related to Internet of Medical Things



Keeping eHRSS and Your Electronic Medical Records Safe from Cyber Security Threats
Cyber security on eHRSS



Building and Experiencing the User-Centric Patient Portal
Patient Portal design and usability review

eHRSS for District Health Centres
A key enabler for DHC service delivery

Guides on Proper and Secure Use of eHRSS
Publicity and education on eHRSS account security

eHRSS Updates
Latest publicity and engagement activities

With the advance in technology, Mr Lai added that another cyber threat evolving in healthcare is related to the use of new and emerging medical devices that collect health data and interconnect with healthcare IT systems through the Internet of Medical Things (IoMT).

“With IoMT, medical devices can generate, analyse and transmit data through the Internet automatically. Although it facilitates data capturing and processing to provide easy reference for HCPs, it creates security threats as every connection can bring in a new attack surface,” he elaborated. If the security of IoMT is breached, the infected devices can be turned into a botnet and attack other computers.

Cyber Security Planning by HCPs

As cyber threats proliferate, Mr Lai urged enterprises, including HCPs, to place more emphasis and resources to improve their cyber security posture and enhance their cyber resilience capabilities.

HKPC has been providing training and consultancy services on cyber security to both public organisations and private companies in Hong Kong. It also manages the government-funded Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) which coordinates computer and network security incident response and provides cyber security advice for local enterprises and Internet users.

HKPC has been providing training and consultancy services on cyber security to both public organisations and private companies in Hong Kong

“Cyber security is not only about technology. We advocate a holistic approach, incorporating the organisation’s business processes, operations and data to manage and mitigate the cyber security risks it faces.”

“It also includes data management and access control to clearly classify data and properly define access rights, as well as communications and disaster recovery mechanisms for organisations to respond and recover expeditiously in times of crisis,” said Mr Lai. He also stressed the importance of raising employees’ awareness on user account management and vigilance on cyber security threats.

“On top of that, the whole security strategy has to be regularly reviewed for compliance and kept updated. Organisations need to conduct security awareness trainings and drills from time to time,” he added.

Noting that some enterprises may not possess cyber security expertise, Mr Lai said that HKPC has been promoting “Security-as-a-Business(SECABiz)”, the inclusion of security solutions in IT vendors’ packaged products as one of the requirements or value-added services. In this way, enterprises are encouraged to install computer systems or software with a higher security standard with a view to preventing cyber attacks.

Use of strong identity verification, such as biometric authentication can help minimise the risk of data breach

Security Measures at User Side

With the Patient Portal of the Stage Two Development of the eHR Sharing System to be launched in 2020, registered patients can access some of their key eHRs through the Patient Portal mobile application (app). Talking about how to protect data privacy and security in the Patient Portal, Mr Lai suggested the use of strong identity verification, such as biometric authentication, to help minimise the risk of data breach.

Fun Quiz

Chance to win a prize

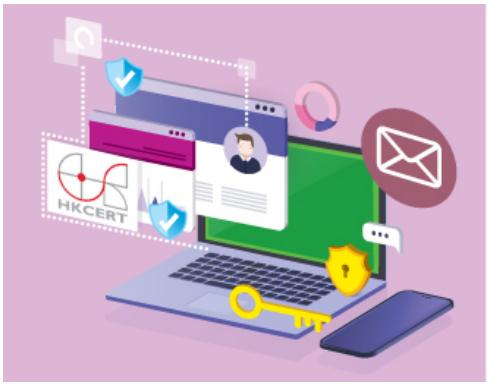
On user side, he highlighted that a good balance between convenience and security should be maintained in order to protect users' health information. Concerted efforts on education and promotion of cyber security are also vital in enhancing the public's understanding on potential security risks and measures to guard against cyber attacks.

He suggested some basic mobile device security measures for users of the future Patient Portal:

- Download the Patient Portal mobile app from the official website or the official app stores
- Avoid logging in the Patient Portal with public devices or in public wifi network
- View and store personal information and eHRs at mobile devices on a need basis
- Never root or jailbreak mobile devices
- Create strong passwords for mobile devices/ wifi routers
- Apply software patches timely
- Update anti-virus software regularly
- Do not open suspicious emails
- Plan for precautionary measures in case mobile devices are lost

New Cyber Security Initiatives for Healthcare Sector

To specifically help healthcare organisations watch out for potential cyber attacks, HKCERT had collaborated with Microsoft Hong Kong to run the "Healthcare Cyber Security Watch Pilot Programme", tapping its international experience and knowledge on cyber threats to early detect attacks targeted at the healthcare sector in Hong Kong.



HKCERT will match the IP addresses provided by participating organisations of the "Healthcare Cyber Security Watch Pilot Programme" with their cyber threat database for compromised systems, inform them of any compromise detected and help them clean up their compromised systems

"We will match the IP addresses provided by participating organisations with our cyber threat database for compromised systems, inform them immediately of any compromise detected and help them clean up their compromised systems. The service is free of charge," remarked Mr Lai and he welcomed all local public and private hospitals, clinics and other HCPs to join the programme.

"All organisations, regardless of industry, location or size, are possible targets of cyber attacks. To increase awareness on cyber security risks in the healthcare sector, HKCERT will continue to keep an eye on the latest development and provide tailor-made trainings and guidelines to assist the industry in detecting, containing and eradicating cyber security incidents," Mr Lai concluded.

Building and Experiencing the User-Centric Patient Portal

The Patient Portal will be launched in phases with initial functions targeted to be rolled out in the second half of 2020. Earlier, five patient and parent groups were invited to join the first round of usability review activities to experience the prototype developed for the Patient Portal and provide feedback.

The Patient Portal is one of the main work targets of the Stage Two Development of the Electronic Health Record Sharing System (eHRSS). In light of the greater emphasis placed on promoting primary healthcare, medical-social collaboration and Public-Private Partnership (PPP) in recent years, the Patient Portal will be playing a greater role and positioned as the public health portal in Hong Kong.

With the above aim, a set of parameters has been drawn up to guide the development of the Patient Portal. Right from the start, development teams have adopted a user-centric design and the agile development approach as major steps to define requirements and improve user experience before the Patient Portal makes its way to the public.

In light of the greater emphasis placed on promoting primary healthcare, medical-social collaboration and PPP in recent years, the Patient Portal will play a greater role and positioned as the public health portal in Hong Kong

Building an Effective Public Health Portal

Positioned as the public health portal in Hong Kong, the Patient Portal is envisaged to serve as an integrated platform or “hub” to provide information and a range of functions that can help engage users and empower them to more actively manage their own health.

Keeping eHRSS and Your Electronic Medical Records Safe from Cyber Security Threats

Cyber security on eHRSS

Cyber Security in Healthcare

Mitigating cyber security risks in the healthcare sector

eHRSS for District Health Centres

A key enabler for DHC service delivery

Guides on Proper and Secure Use of eHRSS

Publicity and education on eHRSS account security

eHRSS Updates

Latest publicity and engagement activities

Expected Functions of the Patient Portal at Initial Launch

In developing the Patient Portal, requirements and solutions are crafted and updated through the collaborative efforts of stakeholders, users and cross-functional teams. Within this framework, user needs and requirements can be aptly identified, and modifications can be rapidly and flexibly made to achieve continual improvements. This will be further complemented by the progressive roll-out of functions under the "mobile-first" strategy and the running of trials where appropriate.

Experiencing the Patient Portal

As part of the collaborative development process, the Electronic Health Record Office has commenced a series of usability review activities to gauge users' feedback and suggestions on the Patient Portal through "hands-on" experience with the prototype. The first round was held at the Central Government Offices on 18 March 2019.

Representatives of five patient and parent groups were invited to attend the usability review activities. They were from the Hong Kong Alliance of Patients' Organizations, Society for Community Organization, the Hong Kong Society for the Aged, the AIDS Concern and the Natural Parenting Network

Fun Quiz

Chance to win a prize

Participants of the usability review activities were introduced the features of the Patient Portal mobile application (app) and invited to try out its functions. Feedback on the design, layout, functionalities and usability was gathered.

Overall, participants were positive towards the design and functions of the mobile app and appreciated its easy navigation and presentation in particular. One of the patient group representatives commented, “The app is user-friendly with clear presentation of texts and images. I can easily navigate and obtain health information in just a few clicks.” Another representative said, “The medication and appointment records are useful, especially for carers of the elderly, as managing all those paper records and appointment slips for them is not an easy task at all.”

Participants welcomed the value-added functions such as the integrated “Doctor Search”. “It is very convenient to find out whether a clinic has joined eHRSS or the Elderly Health Care Voucher scheme. It is also easy to check the balance and transaction history of the latter through a single portal. It will be great if search filters, such as district and clinical specialty, can be provided to help us locate suitable healthcare professionals,” a representative remarked.

Parent representatives found the immunisation records at the Patient Portal particularly helpful. “This is one of the most important health records of our children. It is quite handy to have an electronic copy at the mobile app as back-up and to input the records on our own,” one of them said. Another parent also opined, “The interface is easy to use. It is also convenient for parents and carers to view records of both their children or the carees on top of their own via the same device. Yet, there must be measures to protect data privacy and security.”

Valuable suggestions on enhancing the mobile app were also collected during the sessions. “A patient may have medical appointments scheduled months or even a year later. It would be helpful if patients can input their upcoming medical appointments on the Patient Portal, in addition to those recorded by doctors in eHRSS, and set reminders on the portal,” a participant mentioned.

Apart from suggesting enhancements to the textual and graphical instructions to improve usability, a representative said, “In future, we may consider providing voice direction guide and navigation on the Patient Portal to assist the elderly and the visually-impaired to make use of the mobile app to manage their own health.”

Representatives opined that the Patient Portal mobile app was a good starting point and they looked forward to having more functions and features. “The Patient Portal, with the availability of easily obtainable health information and a wider range of functions, will help promote self-care and health management in the community. I will surely recommend the mobile app to my family and friends,” a participant said.

The Way Forward

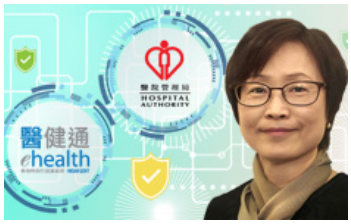
On the whole, representatives of the patient and parent groups were supportive of the design of the Patient Portal and they looked forward to its future development. Users’ participation and contributions are always crucial to the building up of a user-centric Patient Portal. Efforts will continue to be made to engage different stakeholders, including the next round of usability review activities from end-2019, before the Patient Portal goes live by the second half of 2020.

eHRSS for District Health Centres

The first District Health Centre (DHC) at Kwai Tsing came into operation in September 2019, marking a step forward of the Government's commitment to enhancing district-based primary healthcare services. The DHC scheme aims to provide integrated primary healthcare to the public through a network of healthcare professionals (HCProfs) in the localities, under which participants' essential electronic health records (eHRs) are shared amongst HCProfs making use of the Electronic Health Record Sharing System (eHRSS).

Operating through district-based medical-social collaboration and public-private partnership (PPP), DHC is a brand new operation mode in providing one-stop primary healthcare services to the public ranging from health promotion, health assessment, chronic disease management to community rehabilitation.

Under the scheme, DHC serves as a hub comprising a Core Centre as the headquarters in the district, supplemented by Satellite Centres in different parts of the district, as well as multi-disciplinary HCProfs in the private sector such as doctors, Chinese medicine practitioners, dietitians, occupational therapists etc. to provide multiple access and service points for the public. Through the networking approach, it seeks to provide primary healthcare services that cater for the needs and characteristics of individual districts, and enhance public awareness of disease prevention and their ability in self-management of health.



Keeping eHRSS and Your Electronic Medical Records Safe from Cyber Security Threats

Cyber security on eHRSS

Cyber Security in Healthcare

Mitigating cyber security risks in the healthcare sector

Building and Experiencing the User-Centric Patient Portal

Patient Portal design and usability review

Guides on Proper and Secure Use of eHRSS

Publicity and education on eHRSS account security

eHRSS Updates

Latest publicity and engagement activities

eHRSS: a Key Role to Play in DHCs

The effective and smooth operation of the DHC network requires the close linkage and flow of service and client data amongst HCProfs, as underpinned by the eHRSS infrastructure. As in other PPP initiatives, the DHC scheme utilises eHRSS as the information exchange platform to facilitate the delivery of services to its users. Specifically how does eHRSS support the operation of DHCs?

- **Enhancing communication among HCProfs:** Each DHC runs a number of primary healthcare programmes which involve a mix of doctors, allied HCProfs and other workers from the health as well as welfare sectors. Relevant health data of a patient contributed by different HCProfs can be easily linked and communicated through eHRSS to support the provision of more holistic healthcare to the patient. For example, a participating doctor of the Diabetic Mellitus Screening and Management Programme under the DHC programme can make reference to a patient's diabetic retinopathy assessment results conducted and shared in eHRSS by an optometrist in prescribing a treatment and care plan that best suits the patient.

- **Enabling convenient access to health data by public and private HCPs:** eHRSS offers authorised HCProfs ready and secure access to patients' eHRs. In this way, patients' health conditions can be better assessed and followed up by HCProfs, especially for those who have just been discharged from the hospital. For example, the clinical notes of a patient after hospitalisation shared in eHRSS can be viewed by the HCProfs working in DHCs who are responsible for providing rehabilitation services to the patient. This certainly enhances the delivery of continuous healthcare services and coordination among various medical and social service providers in the community.

- **Facilitating efficient operations of DHCs:** The DHC Information Technology System is modelled on eHRSS' Clinical Management System On-ramp with customised functions that provide support to the efficient operation of DHCs, for instance, client registration, eHRSS enrolment, eligibility and medical fee waiver status checking, programme enrolment, service referral and clinical documentation.

It is envisaged that with the progressive roll-out of DHCs, eHRSS would continue to extend its footprint in the community and bring greater synergy to the healthcare services in Hong Kong. For more details about DHC, please visit www.dhc.gov.hk/en/index.html.

Fun Quiz

Chance to win a prize

Guides on Proper and Secure Use of eHRSS

The Electronic Health Record (eHR) Office has recently drummed up publicity and education surrounding the security and management of the Electronic Health Record Sharing System (eHRSS) accounts. Collaterals and guides have been released to strengthen understanding of how to use eHRSS properly and securely.

Patient privacy and data security have always been the top priorities in eHRSS operation, and healthcare providers have indispensable roles and responsibilities in this respect. While eHRSS has built in strong security measures to protect data privacy, every account user and user administrator of eHRSS is obliged to protect the security and privacy of patients' health records by observing proper use and management of their accounts, and accesses to data and information in the system. They need to also beware of and take appropriate measures to guard against potential security threats to ensure that patients' records will not be compromised.

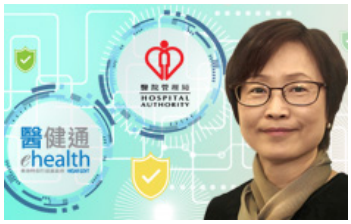
Unauthorised access to eHRSS is unlawful and strictly prohibited

Useful Tips on eHRSS User Account Management

Each authorised user of eHRSS is assigned a unique account for accessing the system according to his/ her roles and duties in delivering patient care. As one of the major rules to safeguard eHRSS data privacy and minimise security risks, a user should access eHRSS only with his/ her own account. Below are some important tips for account users and user administrators -

- Don't disclose or share user name, password and security token
- Keep account login information and security token safe (e.g. avoid writing down the password)
- Report lost security token and suspicious access immediately

- Ensure only authorised healthcare professionals (HCProfs) can access patients' eHRs
- Close the accounts of departed users timely
- Report suspicious access immediately



Keeping eHRSS and Your Electronic Medical Records Safe from Cyber Security Threats

Cyber security on eHRSS

Cyber Security in Healthcare

Mitigating cyber security risks in the healthcare sector

Building and Experiencing the User-Centric Patient Portal

Patient Portal design and usability review

eHRSS for District Health Centres

A key enabler for DHC service delivery

eHRSS Updates

Latest publicity and engagement activities

An e-leaflet highlighting the above messages has been produced for HCPs' reference. Entitled "Keep Your User Account Safe", the e-leaflet can be viewed and downloaded at the eHRSS website.

Cyber Security Tips

To help HCPs protect patients' information and eHRs when using computers connected to eHRSS via the Internet, a new "Cyber Security Tips" corner has been set up on the eHRSS website to provide some useful tips and reference information on cyber security. Apart from general advice, specific tips on the following are covered:

- prevent malware infection
- defend against ransomware attacks
- secure mobile devices
- prepare for security incident handling

Frequently Asked Questions

The Frequently Asked Questions page of the eHRSS website has also been enriched to include common questions from HCPs and HCProfs regarding the use of eHRSS accounts and security requirements. To know more, please visit the below pages -

Use of eHRSS by HCProfs
https://www.ehealth.gov.hk/en/ehr_related_information/faq/healthcare_provider_and_professional.html#use_ehrss_prof

Operation and Security
https://www.ehealth.gov.hk/en/ehr_related_information/faq/healthcare_provider_and_professional.html#operation_security

Fun Quiz

Chance to win a prize

eHRSS Updates

As a continuous effort to publicise the Electronic Health Record Sharing System (eHRSS), the Electronic Health Record (eHR) Office had launched a community roving exhibition together with a series of promotional and engagement activities. New thematic collaterals were also introduced to healthcare providers (HCPs) and patients to enhance understanding of eHRSS.

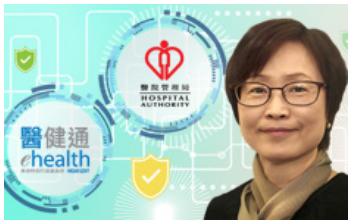
eHRSS Community Roving Exhibition

To sustain the momentum of the one millionth patient registration at eHRSS' third anniversary, a roving exhibition was launched by the eHR Office to further promote eHRSS in the community. The first exhibition was held at the Amoy Plaza in Kowloon Bay (26 to 30 July 2019). Registration counters were also set up to facilitate visitors to register on-site. Close to 770 members of the public were registered during the exhibition.

The concept and benefits of eHR sharing, key features of eHRSS and its latest development were highlighted through display panels and video broadcast at the exhibition. Participants including citizens in the neighbourhood and visitors to the venue were introduced to eHRSS and invited to take part in an interactive fun game to learn more about the system. For upcoming exhibitions, please stay tuned to the eHRSS website.

eHRSS on RTHK Live Programme

eHRSS was presented on air at the live programme "Healthpedia" on Radio 1 and TV 31 of the Radio Television Hong Kong on 5 July 2019. Mr Ian Chin, Principal Assistant Secretary for Food and Health (Health) of the Food and Health Bureau and Dr Clement Cheung, Senior Health Informatician (eHR) Special Duties of the Hospital Authority (HA) attended the interview to share with audience about the latest development of eHRSS, some common questions and concerns about eHRSS participation and the major work areas of Stage Two Development.



Keeping eHRSS and Your Electronic Medical Records Safe from Cyber Security Threats

Cyber security on eHRSS

Cyber Security in Healthcare

Mitigating cyber security risks in the healthcare sector

Building and Experiencing the User-Centric Patient Portal

Patient Portal design and usability review

eHRSS for District Health Centres

A key enabler for DHC service delivery

Guides on Proper and Secure Use of eHRSS

Publicity and education on eHRSS account security

The programme (in Cantonese) is now available online:
RTHK Radio – https://www.rthk.hk/radio/radio1/programme/healthpedia/episode/580743
RTHK TV – https://www.rthk.hk/tv/dtt31/programme/healthpedia_tv/episode/575045

Promulgation at Social Media Platform

To complement the existing publicity channels, the eHR Office had utilised digital marketing more extensively to promulgate eHRSS to a wider range of audience and encourage participation. Since May, Internet users would find eHRSS appearing at popular social media platforms such as YouTube and the Google Search Engine and Display Network. Through these platforms, viewers would be directed to the promotional videos where they would find more information about eHRSS and links to online registration at the eHRSS website.

eHRSS Briefing for Expectant Parents

At two seminars jointly organised by the Department of Health and the Natural Parenting Network held at the Hong Kong Central Library on 16 May 2019 and 24 August 2019, representatives of the eHR Office and HA had the opportunity to introduce to close to 200 expectant parents and other carers about eHRSS, in particular its benefits to newborns and children. Participants were encouraged to join eHRSS and to register their newborns early to facilitate the building up of life-long health records.

User Forum on Radiology Image Sharing

To prepare healthcare institutions currently taking part in the Radiology Image Sharing Pilot of HA to migrate to radiology image sharing under Stage Two Development of eHRSS, a forum was organised on 20 June 2019 at the Centre of Health Protection. More than 110 healthcare professionals (HCProfs) and representatives from the private hospitals, radiology centres and groups attended the event. Participants were updated on the development of radiology image sharing through eHRSS and briefed on the preparation work, technical requirements and migration plan.

Fun Quiz
Chance to win a prize

Seminar on eHRSS Latest Development

A seminar themed “Understanding eHRSS – New Milestone New Horizon” was held at the HA Headquarters on 13 September 2019 for healthcare providers (HCPs) from both the public and private sectors. The event comprised a suite of presentations by representatives of HA, sharing with participants about the latest development progress and milestones of eHRSS, easy and smart ways for utilising the system, tips on privacy and security protection and other best practices. Over 300 HCProfs, administrators, information technology and management staff of eHRSS participating HCPs and interested organisations attended.

New eHRSS Collaterals

New collaterals covering the following aspects of eHRSS were designed and disseminated to HCPs and patients:

- Benefits and use of eHRSS for patients on admission to public hospitals: The leaflet aims to introduce eHRSS and explains about the arrangements of upload and access to eHRs for in-patients of public hospitals.

- Role-based access control (RBAC): The poster and leaflet illustrate eHR access opened to different groups of HCProfs under the RBAC mechanism, and the privacy protection and data security controls that are in place. For more details, please refer to “Extending Role-based Access to Allied Health Professionals in the Community”.

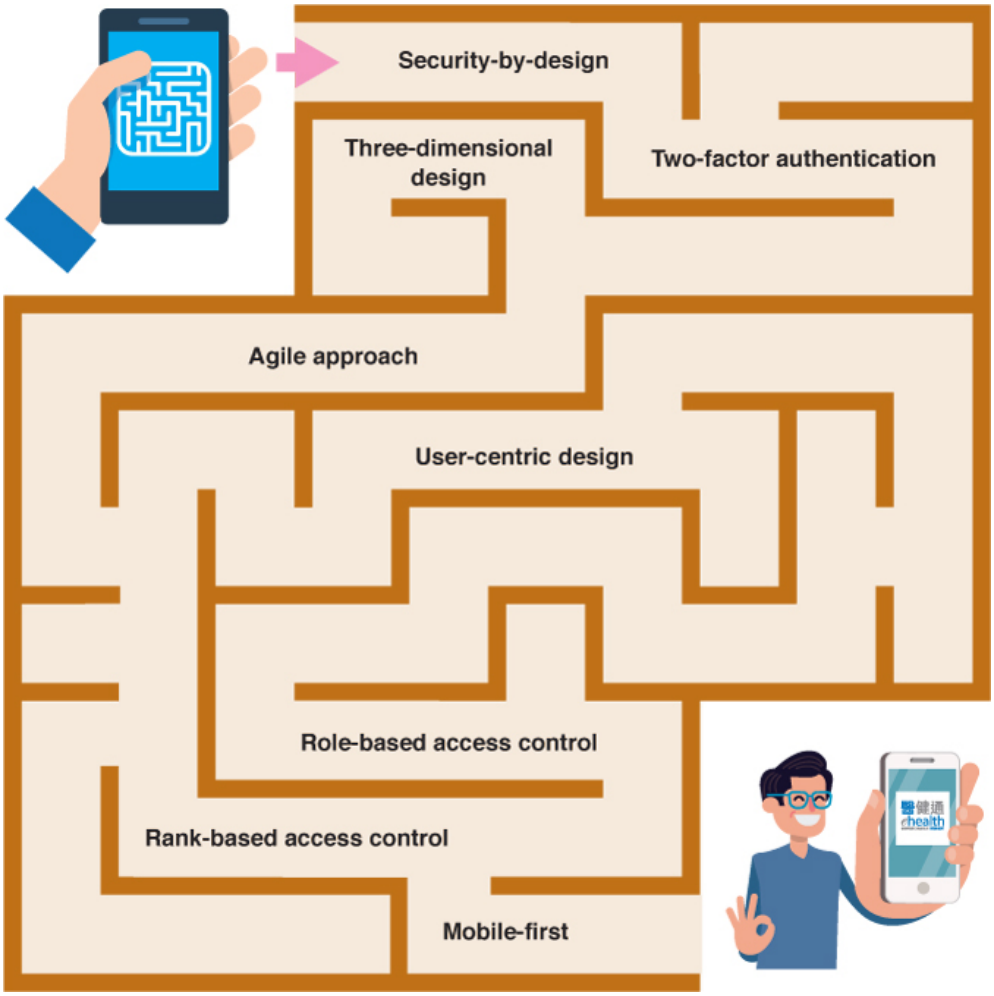
- Scope of eHRSS sharable data: The leaflet features the nine types of data that can be shared among HCPs with patients’ consent under Stage One eHRSS.

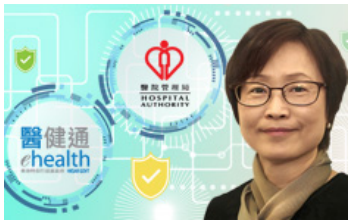
Fun Quiz — Chance to Win a Prize

Maze Game

The development of the Electronic Health Record Sharing System (eHRSS) has been following a set of principles and approaches. In the maze game below, find them out by drawing a line from the starting to the finishing point. Ultimately it will show the correct way out of the maze.

Winners will receive a prize, while stock lasts. (Hint: The answers can be found in this issue of eHealth News.) Enjoy and don't get lost!





Keeping eHRSS and Your Electronic Medical Records Safe from Cyber Security Threats

Cyber security on eHRSS

Cyber Security in Healthcare

Mitigating cyber security risks in the healthcare sector

Building and Experiencing the User-Centric Patient Portal

Patient Portal design and usability review

eHRSS for District Health Centres

A key enabler for DHC service delivery

Guides on Proper and Secure Use of eHRSS

Publicity and education on eHRSS account security

Join the Quiz

To join the quiz, please print out this page, mark your answers and fill out the required information. Completed entries should be returned by fax at 2300 7921 or email to enquiry@ehealth.gov.hk on or before 6 December 2019.

Name :			
Tel. no. :		Email :	
Address :			

After the closing date on 6 December 2019, you can check the correct answers in the eHealth News posted at the eHRSS website. Personal particulars and contact information collected in this fun quiz will only be used to notify winners and send prizes. All personal data collected in this fun quiz will not be disclosed to any third parties and will be deleted by the Electronic Health Record Office two weeks after all prizes have been sent.

eHRSS Updates

Latest publicity and engagement activities