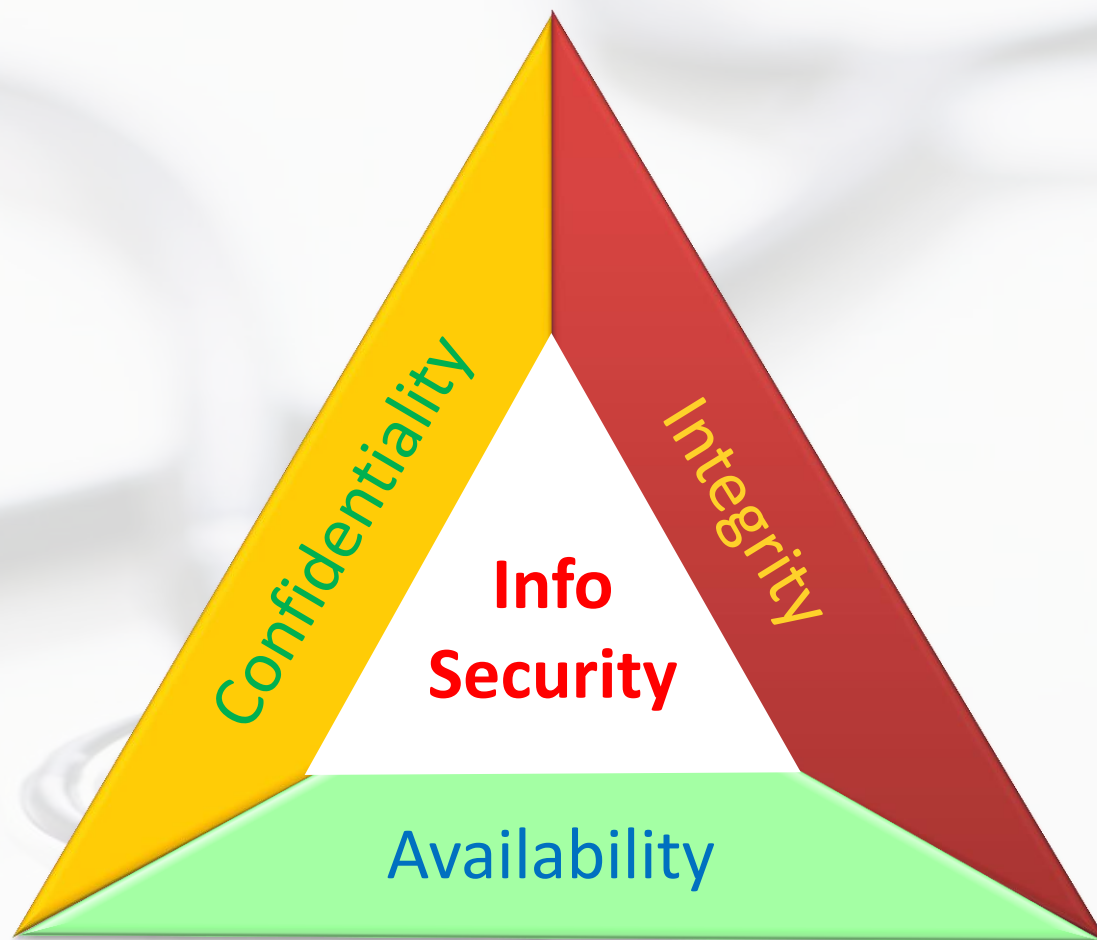


Keep eHRSS & your EMR Safe from Cyber-attacks

Clara Cheung
Chief Systems Manager
Hospital Authority



‘Inadvertent Weakness’

- Fall for Phishing
- Use of Weak Passwords
- Unsecured Personal Devices
- Delayed security patches, outdated software
- Poor security mindset

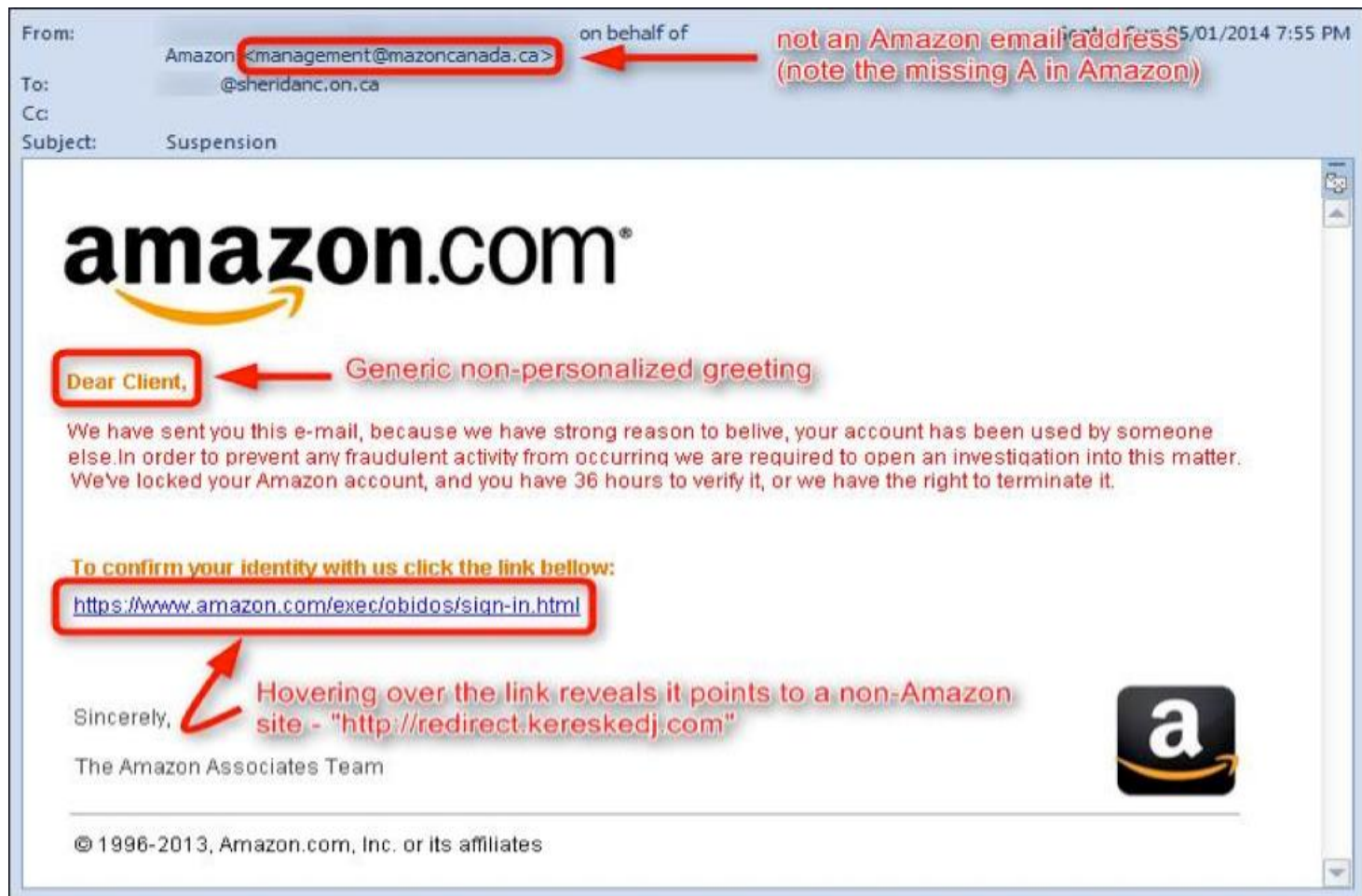
What you can do

- Be suspicious

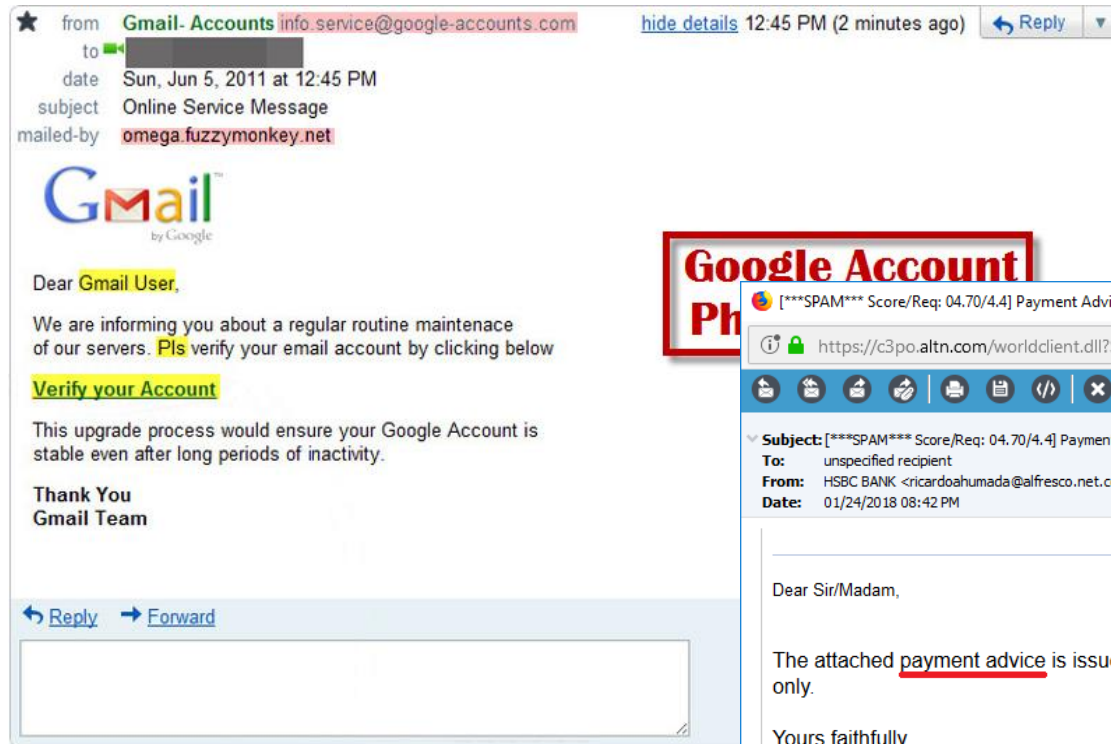
What is Phishing

- **Phishing** is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
 - Compromised Credentials
 - Dropping Malware
 - Business Email Compromise (CEO Fraud)

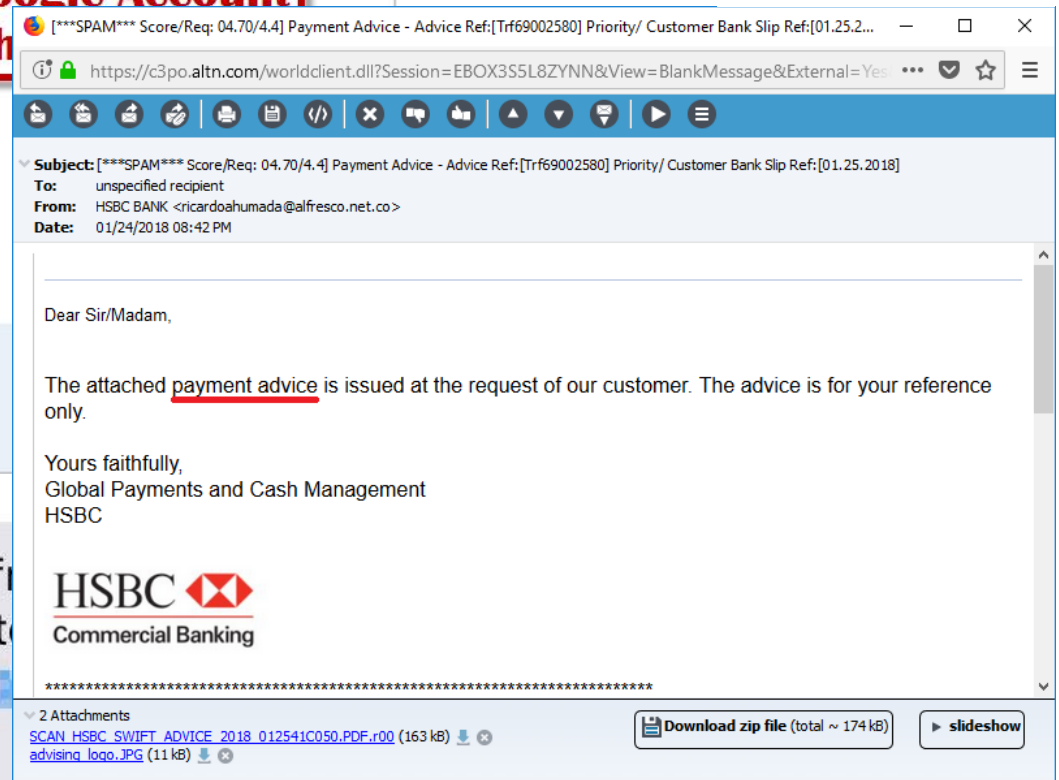
Be Wary of Suspicious email/messages



Think before You Click



Google Account
Ph



You have a refund pending from HMRC. Use our secure link to update your details for payment:



Learn Who to Trust



https:

View Certificate

The screenshot shows the eHealth.gov.hk website with a browser window. A pop-up window titled 'Website identification' is visible on the left, showing the site's identity and a 'View certificate' button. The main website content includes the 'Electronic Health Record Sharing System' header, navigation menus, and a large banner for 'HCP Number' search. On the right, a 'Certificate Information' panel displays details about the website's SSL certificate, including the issuer (Hongkong Post e-Cert CA 1 - 15), validity dates, and the subject organization (Hong Kong SAR Government).

Website identification

Hongkong Post Root CA 1 has identified this site as
www.ehealth.gov.hk
Hong Kong, Hong Kong

Your connection to the server is encrypted.

[View certificate](#)
[Should I trust this site?](#)

Website permissions

You haven't set any permissions for this site yet.

[Allow Adobe Flash](#)

醫健通 ehealth 電子健康紀錄互通系統
Electronic Health Record Sharing System

Home | Sitemap | A A A | 繁體 简体 Eng | Mobile Version

Enter search keyword(s)

About eHRSS **Patient** **Healthcare Provider and Professional** **Ordinance and Related Information** **Information Standards** **Training and Partnership** **Publicity** **FAQs and Forms**

Location **Registration Centres** **HCP Number**

Search for Registered Healthcare Providers

Patient

- Register Myself
- Register My Child
- Register a Person Incapable of Giving Consent
- Activate My eHealth Record
- Registration Forms
- eHR Registration Centres
- Mobile Registration Team

Healthcare Provider and Professional

- Registration
- How to Register
- Registration Forms
- Supporting Documents
- IT Requirements
- How to Obtain Access
- Code of Practice

Certificate Information

Hongkong Post Root CA 1

Hongkong Post e-Cert CA 1 - 15

www.gov.hk

www.gov.hk
Valid Certificate

Issued by
Hongkong Post e-Cert CA 1 - 15

Valid from
15 October 2018 11:09:54

Valid to
20 October 2019 17:35:12

Subject organisation
Hong Kong SAR Government

Subject locality
Hong Kong, Hong Kong

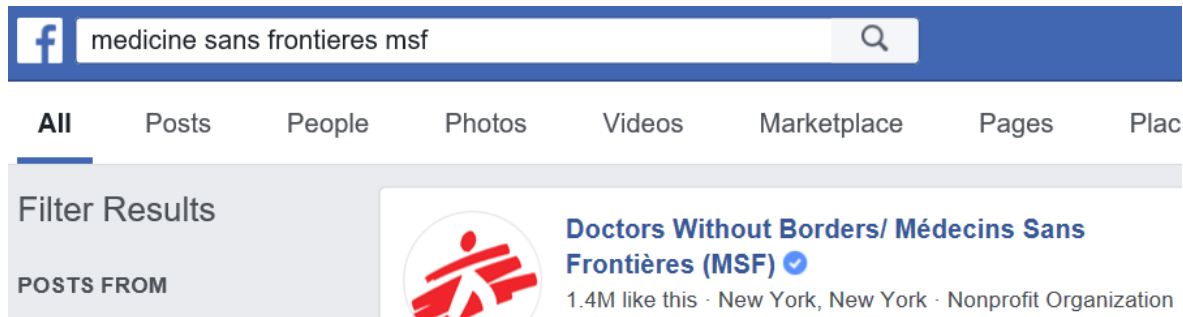
Subject country
HK

Serial number
6C:87:CD:23:74:54:B5:ED:EF:51:66:F0:94:46:4D:2C:06:9D:8F:B0

SHA-256 fingerprint
13:14:97:41:55:28:D7:34:95:B7:36:5E:19:AD:77:26:02:51:27:3C:B8:15:CF:D3:5E:31:40:03:20:5C:CO:80

[Export to file](#)

Beware of Identity Spoofing



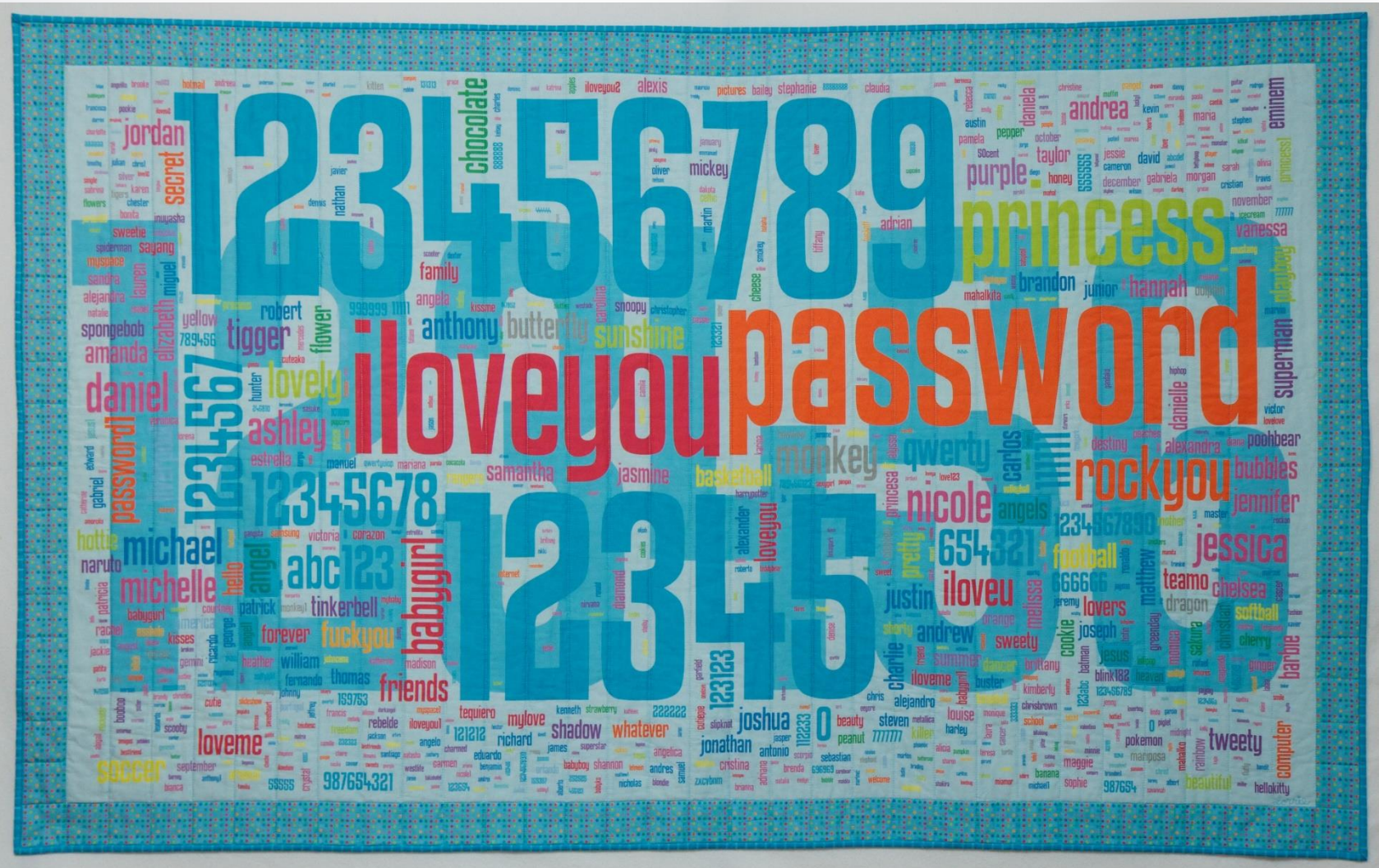
What you can do

- Protect your account

Protect Your Account

- Separate professional & personal accounts ★
 - Do not use same user accounts and passwords for everything
- Distinguish ‘serious business’ vs. ‘fun’
- Develop your own method to help you remember the different accounts and passwords

Weak Passwords



What is Strong Password?

- Never disclose your passwords
- Use long password (passphrases)
 - “ipreferpassphrasesoverpasswords@”
 - easier to remember & more difficult to crack
- If limited by no. of characters, use combination of unrelated words, numbers, special characters (# @ ! | }...), capitals
- Do not use dictionary words or anything personal, e.g. own name, pets’ names, date of birth ...
- Get Creative with Security Questions
 - For increased security, lie about your answers or use passphrases as the answers

Manage your eHRSS Accounts

- Do not share accounts
- Do not disclose your passwords
- Keep your token safe
- Keep an eye on who is watching when you login
- Logout when you won't use the system for a while
- For healthcare professionals, when you leave an employer
 - No need to return your token to your employer (can return to eHRSS Registration Office)
 - Change your password before you leave

What your organisation can do

- Control access to your systems

Manage Authorised eHRSS Accounts

- Do not allow sharing of accounts
- Assign appropriate user roles
- Install ELSA only on authorised workstations
- Check eHRSS User Access Log regularly
- Review your list of active accounts regularly
- When an employee leaves
 - ‘End the relationship’, or Terminate the account

Role Assignment

Close

Role Group Assignment

Assign Role Group to HCS

Assign/View Role Group to HCP

Edit Admin Role Group

User Information

eHR UID:

2466794707

User Name:

donalddto

Account Status:

Active

Relationship Information

HCP	Relationship Type
VHA HOSPITAL - 3098159131	Prime

HCP Selection

The HCP selected:

3098159131

HCP:

VHA HOSPITAL - 3098159131

Assign Role Group Information

Role Group Start Date*:

21-Jan-2019

Role Group End Date:

dd-MMM-yyyy

Role Group

<input type="checkbox"/>	Allergy and Adverse Drug Reaction (ADR) Input Module	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Call Centre Agent	<input type="checkbox"/>
<input type="checkbox"/>	Clinical Data Admin - User Admin	<input type="checkbox"/>
<input type="checkbox"/>	Clinical Professional	<input type="checkbox"/>
<input type="checkbox"/>	Clinical Professional (Full)	<input type="checkbox"/>
<input type="checkbox"/>	CRC CLUSTER ADMIN (HA)	<input type="checkbox"/>
<input type="checkbox"/>	CRC CS Doctor	<input type="checkbox"/>

End Relationship

Manage User Account IVRS Log

Create New User Account

Healthcare Provider: VHA HOSPITAL

Personal Information

ID Doc Type*: HKID Card

HKIC No.*: V000581 9

Surname*: TO

Given Name: DONALD

Chinese Name:

Contact Phone No.:

Post Title:

Title (English):

Contact Person: ☐

Fax No.:

Title (Chinese):

Contact / Notification Information

Communication Means*: Please Select

Internet Email Address*:

Mobile Phone No.:

Re-enter Internet Email Address*:

Administrative Institution

Healthcare Service Location*:

Name	Contact No.	Address
------	-------------	---------

Login Information

User Name*:

User Name must be 6 to 20 alphanumeric characters

Second Authentication Factor*: Please Select

Token / e-Cert / Mode A is required for:
1. Healthcare Professional to view eHR record
2. User Admin to manage user account

Relationship Information

Healthcare Staff Type*: Please Select

Relationship Start Date*: 21-Jan-2019

Relationship End Date*: dd-MMM-yyyy

Create Back

What your organisation can do

- Protect your Systems and Data

Protect Your Assets

- Back up valuable data
- Beware of unsafe storage devices
 - Do not connect other people's devices to your computer
 - Run antivirus scan, even if it is new, on a computer not connected to the network nor the internet
- Enforce screen saver with passwords
- Secure physical and cloud storage
- Learn to manage configurations of your EMR
- Password lock files with sensitive information
- Disable 'Guest' Login

Software Security

- Keep your software up-to-date (Browser & OS)
 - Backup your data and system before update / patches
- Use anti-virus & anti-malware & keep definitions up-to-date
- Check security features of your EMR
 - Require mandatory user login to system
 - Enforce clear delineated roles and access for different types of users
 - Support and enforce strong passwords
 - Encrypt sensitive data in transit and storage
 - Support current OS and Browser versions
 - Provide auto time-out or screen lock

Beyond electronic medical record

Security Mindset

- Security Awareness Training
- Lock up paper records / photocopies with personal data
 - Who will be there after-hours?
- Check twice before giving out patient reports
 - Aware mixing up photocopies
 - Aware mixing up patient identities in reports
- Place workstations appropriately to avoid prying
- Secure your backup storage