Mobile health application

Technology, Information Technology

Mobile Health Application Insert Insert Security and Privacy Threats on Mobile Health Technologies Introduction Mobile health technologies are software application programs formulated to offer health services via mobile phones (smartphones) and tablets (Remedy Health Media, 2014). Many apps have been created and incorporated into the field of medicine to enable medics regularly get in-touch with their patients despite the location and time (Brookings, 2013) due to these many reasons many apps have been created including Medscape, Epocrates, My Heart Care and much more apps.

Medscape app

Medscape is a medical app most used by physicians, nurses and medical students due to its complete and widespread medical applications. It is a small book for not only drug reference but also has several rules for disease pathologies. Medical students and professionals like Medscape because it has instructions on performing medical procedures, videos on the actual action and detailed pictures (Sullivan, 2013).

Many because of free content also love it; over 7, 000 drug orientations, 3, 500 disease medical references and medical images about 2, 500 are all free on the app. Strong drug interaction tool checker CME activities are also some features that make Medscape more favorable. The app regardless of features achieves the application in mobile phones and tablets. It can be accessed offline without the internet connection; you only download the medical reference database (Schulk, 2013). The idea is almost real to everyone since almost each person owns a smartphone (Dalrymple, 2010). Despite all the benefits acquired from the app, it also has disadvantages especially on

security and privacy threats. Some of the threats include:

Stolen mobile device- in case the mobile device which was actively used to access, transmit and eventually store patient's information on his/her health gets lost or is stolen, the patients data might be at great risk of getting into wrong hands. The culprits might alter the medical information, and this may pose a great risk to person's health. In addition, medical identity theft may occur whereby another person uses a person's name and medical number (Dixon, 2006). To avoid all these, all mobile devices used by medics must be designed to ask for passwords, special codes or fingerprints in order to gain access. Area for entering passwords must be masked so that a person cannot see it avoid cracking of the password. Remote wiping or disabling can be activated on the device, which can allow erasure of all information on the device in case it is lost or stolen and if later recovered data can be recovered by enabling the device.

Using public Wi-Fi network- Wireless Fidelity is a means of the device/mobile connectivity and enables data transfer (Mitchell, 2010). Patient's health information can be transmitted or stored on the mobile device using unsecured Wi-Fi network. The information might pose a risk of breach by a third party on the network. The information/ patient's data may be secured by encryption. Data encryption is making data unreadable, unintelligible unless one has a code to decrypt that data.

Securing your mobile device on the network- patient's information must be a number one priority to physicians to ensure true and efficient information to and from the patient with no other party interference. Passwords, and log in details must be in use to avoid third party accessing patient's data in case

another person handles the device. Firewalls and security software must be put in place to prevent unauthorized access to information on the network (Healthit. gov, 2015).

References

Healthit. gov,. (2015). Identifying Mobile Health Security Risks in Your Practice | Providers & Professionals | HealthIT. gov. Retrieved 23 February 2015, from http://healthit. gov/providers-professionals/dr-andersons-office-identifies-risk

Sullivan, H. (2013). Symptoms app MedscapeMobile app £2. 49. Nursing Standard, 28(11), 31-31. doi: 10. 7748/ns2013. 11. 28. 11. 31. s38