HealthManagement
Promoting Management and Leadership

New UK IT cybersecurity rules

In this age of digital communication, healthcare organisations face new challenges in protecting sensitive patient information. Within NHS trusts, for instance, consumer messaging apps like Facebook Messenger and WhatsApp are now widely used by staff for sending or sharing patient data.

Amidst this widespread app use, the U.K. NHS recently issued new instant messaging guidelines for clinicians in the acute care setting, including privacy policies for sharing patient data. The NHS guidance sets standards for determining whether an app is safe to use in the healthcare setting. This includes only using apps with encryption standards, end-user verification and passcode protection.

The guidelines also require clinicians to only use apps that can be remotely wiped in case of loss or theft, along with message retention features that delete messages after a set amount of time. Moreover, the guidance says these apps should only be used if an organisation doesn't provide a suitable alternative.

The new guidance was released following a damning CommonTime report that found the majority of NHS trusts lacked official policies regarding the use of instant messaging (IM) apps. Of note, 97 percent of clinicians routinely used those IM apps to send patient data without those security measures in place, according to the report.

"Instant messaging can have clinical utility but remember that the law places obligations on organisations to protect patient confidentiality," according to the NHS guidelines. "If you are a clinician, you may also have to defend yourself against regulatory investigation if you have not taken sufficient steps to safeguard confidentiality."

Those safeguards include keeping clinical records separate from the app and deleting patient notes after they've been transcribed into a patient's medical record. Clinicians should also avoid sharing devices and ensure lock-screen notifications are disabled.

Other measures included in the NHS guidelines are:

- Clinicians should ensure that they are communicating with the correct person or group, as there are often similar names stored in an address book.
- IM group administrators should also routinely review membership.
- The app is not linked to any other platforms, especially social media or a device's photo library.
- Social groups must be separate from the clinical or operational information.
- Two-factor authentication is required.

The guidance is just the latest security measure enacted by NHS following more than a year of security incidents and troubling reports.

NHS was crippled by the global WannaCry attack in May 2017, after failing to patch a known vulnerability. Nearly a year late, all 200 NHS trusts failed a government security audit – many for failing to patch known flaws. Also, in August 2018, a report from think tank Parliament Street found NHS lost 10,000 paper patient records last year.

Source: NHS Digital; HealthITSecurity.com
Image credit: Pixabay

Published on : Tue, 20 Nov 2018