HealthManagement.org
Promoting Management and Leadership

Is Your X-ray Machine Scuppering IT Security?

This year alone has seen a huge increase in cyber attacks on healthcare data. It is no coincidence theta cybercriminals target healthcare. While compared to other sectors, the financial gains of hacking into a hospital's data and demanding a ransom for release, are negligible, the guarantees of success are greater.

For one thing, many healthcare facilities are operating under old IT applications using older systems that are much easier to penetrate than those in the financial sector for example. For another, hackers know that a hospital will probably fold under the pressure to release data as in some cases patient lives depend on it. Reputation always does.

A report in Health Data Management takes look at two of the most common weak points that hackers take advantage of and what healthcare executives can do to minimise the risks.

First Line of defence: Doctors

With medical charts now beings stored electronically, physicians hold the keys to access to patient data. Surprisingly, many doctors still don't understand that simple actions – or lack of them – can seriously compromise the security of such data.

In order t spend more time with a patient or to move onto the next task, sometimes doctors forget to log off their computers. Using weak passwords for easy remembering rather than employing a range for different systems also contributes to making data more vulnerable to hackers.

Naturally, hackers have exploited these tendencies and targeted healthcare records. In light of this, proper security awareness for all staff members is essential including remedying the above practices. Training should also highlight not clicking on suspicious emails or visiting sites that may comprise security.

Following training, reminders to implement security practices are necessary.

See Also: **Cyberhygiene Best Remedy Against Healthcare Hacking**

Confirm Who is Responsible for Devices

Who owns the digital X-ray machines or electrocardiograms in your healthcare facility? Sometimes it is the vendor. This leaves healthcare providers vulnerable to external breaches that are not covered by in-house standards. Sometimes it is medical staff themselves who are responsible for maintaining standards. In order to ensure hat such devices are as secure as possible, hospital executives must monitor who has access to them, be crystal clear on the security standards imposed by the vendor and pinpoint practices to maintain stringent levels of security. It is no exaggeration to say that such practices could make the difference in a life or death situation.

Source: Health Data Management

Image Credit: locutushealth

Published on : Tue, 4 Oct 2016