HealthManagement
Promoting Management and Leadership

Healthcare Data Breaches

There have been several news stories recently related to sophisticated data breaches of confidential data in hospitals and healthcare organisations. Early this year, two healthcare organisations lost tens of thousands of data records because of lost USB flash drives and data sticks. The extent of data breaches was large enough to cause the HIPAA to require that all such incidences be listed on the data breach website of the Department of Health and Human Services.

According to a news story reported by U-T San Diego, personal information including names, dates of birth, diagnoses, treatments and insurance information of nearly 5,000 patients was stolen last month from Palomar Health. The data included 36 Medicare identification numbers. While the stolen data included no specific medical records or financial information, personal information was exposed. It is believed that someone swiped a company laptop and two flash drives from an employee's car.

The Role of Mobile Devices

A primary reason for the increase in data breaches is the excessive use of smartphones as well as the increasing number of employees who take office laptops and tablets home. While access to these devices is considered to have a positive impact on productivity, it can also be risky, especially in cases when the data are not encrypted.

However, all blame cannot be placed on devices that are taken home since the same devices can be (and have been) stolen from offices as well. In fact, a data breach at Santa Rosa Memorial Hospital affected nearly 33,000 patients. Data were stolen when a computer thumb drive with information on patients' X-rays went missing from an outpatient imaging centre.

Apparently, the drive had gone missing from the locker of a staff member who had backed up these records on the drive with the intention of migrating the data to Santa Rosa Memorial's electronic medical records system. Comprehensive information was stolen including first and last names, gender, medical record numbers, dates of birth, dates and times of service, area of the body images, names of the X-ray technologists and radiation levels required to produce the X-ray.

Cloud Considerations

These recent breaches indicate that unencrypted flash drives and data sticks are too risky, especially in a hospital/medical setting, because data generally contain personal and confidential patient information. It would be a much safer practice to store such confidential data in secured clouds where it can be accessed by authorized devices only. Data should be encrypted and access controls strictly enforced. This can go a long way in ensuring data are safe whether the device is at the office or at an employee's home. Not only will employees enjoy the benefit of having access to important data 24 hours a day, but the safety and security of these data would also be ensured.

Source: Accellion.com
Image Credit: Globalnews.ca

Published on : Sun, 7 Sep 2014