HealthManagement.org
Promoting Management and Leadership

What gives CIOs insomnia?

In a recent forum organised by LexisNexis, 30 high-level executives, most of whom were CIOs from U.S. hospitals, nursing homes and health plans of all sizes, tackled key data-related issues that are keeping them up at night. Based on the discussions, CIOs are keenly aware of the security complications that medical devices and telehealth bring.

Here are six areas CIOs said they are focused on in 2018.

1. Interoperability

Described by many of the participants as a “daily challenge,” interoperability affects their ability to exchange data, such as patient EMRs. Yet the executives struggled to even come up with a unified definition of what interoperability is. For some it was about sharing records for provider referrals and different settings of care. For others it meant surfacing relevant medical history data to the right specialist and not just passing on a record and helping those specialists filter through the data to get to what’s most important.

2. Security

As more devices are added, the amount of security needed is increased. Thus hospitals are always looking for ways to upgrade security and make sure their data isn’t breached. They talked a lot about digital platforms like portals, telehealth and how to make those more secure. The balance between being asked to make data more readily available to patients but at the same time putting security in place to keep data protected is a constant focus. Finding that balance is a challenge.

3. Identity authentication

CIOs know that providers aren’t necessarily seeing the patients in person anymore. They’re logging on and doing more self-service activities online, even checking lab results online. So how do you verify they are who

they say they are before you provide them with medical care and advice and access to their records. Remote authentication therefore is top of mind.

4. National patient identifiers (NPI)

This was one issue on which all the participants seemed in full agreement. “We need it” was the overwhelming consensus and there was surprise that hasn’t been more federal money spent on establishing one considering the widespread acknowledgment that it is necessary and important. Would help with interoperability, especially in light of M&A activity where systems are having to merge disparate systems. “An NPI would help with this because today each system uses its own algorithm and their own identifiers so it may work within that system but when they try to move information outside the system it starts to add complexity into the process.”

5. Patient record linking

Errors in patient identification pose a threat to patient safety and are therefore an unending concern. Mismatching patients and records can lead to missed diagnoses and incorrect treatments. The ongoing digitisation of health records means the volume of data is swelling and this issue will only get bigger.

6. Provider directory

According to the executives, keeping their provider directories current is an ongoing issue. They know that provider data is continually changing and most admit they have limited resources assigned to handling updates. The information is constantly changing, with 50 percent of information in directories becoming out of date after 18 months. On the provider side, just one practitioner’s office might contract with several different carriers and associated plans and they have to go through and update that info by email or fax to each one as frequently as every month. Those updates can happen at different times so for an office staff it can be a daunting task.

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Tue, 10 Apr 2018