COSMOS
Navigate the Compliance Universe

Compliance Today - February 2018
Digitally protecting patient information

by Eric Anderson

Eric Anderson (eanderson@clearwaveinc.com) is COO of Clearwave in Atlanta, GA.

Digital healthcare technologies, like those powered by artificial intelligence (AI), are transforming patient-provider interactions — and 66% of healthcare executives believe some of these innovations fall into a gray area of regulatory compliance.[1]

The trends extend even beyond that of telemedicine, smartphone applications, and wearable technology. Today, virtual assistants like Amazon's Alexa not only answer consumers' health questions, but have also been trained by the American Heart Association (AHA) to recite instructions for CPR in an instant. Meanwhile, according to a recent survey, 63% of healthcare organizations now use cloud-based clinical applications to fulfill the need for scalable, flexible, and reliable infrastructure solutions.[2]

Five steps to protect patient information

As an increasing amount of patient information is processed digitally, healthcare providers face new challenges and opportunities related to compliance. Here are five ways healthcare organizations can better protect the security of patient information using digital technologies.

Eliminate paper-based processes

A recent HIMSS survey shows 90% of clinicians still use paper-based documentation, and most front offices still rely on paper-based check-in.[3] This puts patients at risk for identity theft, especially when papers are left unattended at the front desk. It also presents issues related to HIPAA compliance.

Technologies that support digital check-in enhance the security of patient information by capturing the information electronically, limiting the number of people who touch or view patients' personal data. Often, the information is entered by patients themselves in a waiting room or, in some instances, from their home via their mobile device. Some models automatically update changes to patient information in the organization's electronic health record (EHR), eliminating the need for manual updates by front desk staff. This further protects the privacy and security of sensitive patient information.

Verify patient information in real time

It's not uncommon for patients to make a mistake while providing personal information to front desk staff, whether by hand or electronically. Transcription errors further exacerbate the problem as staff attempts to read and type in data from paper forms. Advanced technologies that verify patient demographic and insurance information with third-party sources and allow patients to correct data at the point of check-in vastly improve data accuracy. Such technologies also ensure the right patient is matched with the right medical record throughout the continuum of care, supporting best practices for verifying patient identity under HIPAA. In addition, they can raise a red flag for front desk staff when the identity of the patient may be in question.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

Enable patients to sign consent forms electronically

A study published in *JAMASurgery* found 66% of scheduled surgeries are missing a critical consent form or final approvals — and 14% of surgeries are delayed because of this.[4] Technologies that support electronic signing of necessary consent forms provide the following advantages:

- Forms are stored in the patient's EHR.
- Time and date of signing is automatically captured in accordance with compliance requirements.
- Electronic access to consent forms ensures patients are signing the most up-to-date forms.
- Forms are automatically populated with patient-specific information and the risks associated with the patient's procedure or service, further supporting compliance.

Communicate securely with patients

Some of the most exciting advancements in digital health are those that improve patient compliance with treatment regimens and medication adherence by enhancing communication between providers and patients. For example, tuberculosis patients in three California counties use a medication management app provided by public health officials to remind them to take their medications. One company has even developed facial-recognition technology that documents medication has been taken.

In a consumer-driven healthcare environment, digital tools that enable providers to securely and instantly communicate outside the traditional care setting offer the ability to protect patient information while supporting improved outcomes. When weighing the benefits of such technologies, look for HIPAA-compliant service providers, and carefully consider the types of information that will be exchanged between patients and providers. It's also important to obtain informed consent from patients prior to taking a digital communications approach.

Add extra protection with cloud-based security

Healthcare cybersecurity attacks are on the rise, yet three out of four hospitals do not have a designated IT security person on staff, according to the U.S. Department of Health and Human Services (HHS).[5] Cloud solutions offer added protection against medical data theft by providing access to the latest IT security applications as well as advanced options for data backup and recovery. They feature encryption technology that protects data in transit and at rest. It's an approach HHS is adopting at a quicker pace, with plans to move 41% of its data to the cloud by the end of 2017.[6]

This document is only available to members. Please log in or become a member.

Become a Member Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.