Patient Access Playbook: The world of apps

APIs and patient apps

The Promoting Interoperability (PI) Programs require certified electronic health record?(EHR) technology to include advanced programming interfaces (APIs) that allow for secure communications between apps.

When you complete your taxes online, an API may allow your online tax software to seamlessly pull information from multiple bank accounts after you share your bank accounts' credentials. In health care, the similar promise of APIs is that a patient can use an app on their smart phone to seamlessly pull medical information from numerous health care providers' EHR systems through APIs. APIs can also allow for automated transmission into EHRs—something that can benefit both patients and their care team.

For example, a patient may use a smart-watch to track their fitness and vital signs and various applications on their smart phones to track health-related activities like their nutrition and medication refills. If all these mechanisms utilize API technology, the patient will be able to condense all of this data into one location and make it available to their care team. From the point of view of a physician, this data can be useful in diagnosing an ailment, monitoring treatment effects, and tailoring recommendations to fit the lifestyle of the patient.

Privacy and security of patient apps

In today's world,?even as APIs offer great access and convenience to those who use them, health data privacy should be top of mind. One significant concern with patient apps is the privacy and security of such apps. Is the app developer selling the patient's health information? Will the patient's information be encrypted? What if the patient's mobile device is lost or stolen? Is the health care provider liable for sharing information with an unsecured app? If a patient requests that you share information through an app, you are required to do so under HIPAA and information blocking regulations if you have the technology to do so. Your EHR's API should allow the app to connect and receive information securely, though if there are credible concerns about security, you may have an alternative to allowing the app to connect. You are not responsible for whether the app is a "good

one," including whether it has appropriate privacy and security in place. If the patient's information is breached once stored within the app, you are not responsible.

Nevertheless, it is a good idea to educate your patients about app privacy and security. Many patients assume their medical data are protected by laws when accessed by mobile apps. However, this is not the case. Encourage them to check the health app's privacy policy before downloading it to help ensure that their information will not be misused. Suggest that they password protect their phone if they are going to store medical information on it. Remember, unlike a stolen credit card number, medical information cannot be changed.

Download the playbook

The Patient Access Playbook (PDF) focuses on dispelling HIPAA myths and helping physicians understand their obligations to provide patients with access to their health information.