About APIs

The Office of the National Coordinator for Health Information Technology

Introduction

Thank you for exploring this program about how Application Programming Interfaces, or APIs, can support health information exchange and interoperability. This program is designed for health care providers and patients who are unfamiliar with APIs and want to learn more. By the end of this program, you should have a basic understanding of APIs and will be familiar with some of the technical terms developers commonly use when talking about APIs.

This program is brought to you by the US Department of Health and Human Services' Office of the National Coordinator for Health Information Technology, or ONC. Part of ONC's mission includes developing policy that promotes providers' and patients' ability to exchange health information electronically in collaboration with the health information technology industry. This program explains how APIs can be used by patients and health care providers to exchange health information.

The program will advance automatically from section to section. You can also use the menu to navigate each section.

The Resources tab includes support materials and sites for additional information about APIs.

Side captioning and subtitles are also available.

APIs Can Revolutionize Health Care

In 2015, ONC recognized the potential for APIs to revolutionize health care data sharing, as it has already revolutionized data sharing in other industries. ONC issued a regulation that included "certification criteria" for APIs. Using APIs as part of electronic health records systems, or EHRs, can make it easier for patients to get and share important health information. APIs can also help health care providers share patient information with other providers securely and efficiently.

What Is an API?

APIs are messengers or translators that work behind the scenes to help software programs communicate with one another. If you have ever used a web-based

application or a mobile “app” on your computer, smartphone, or tablet to purchase a flight or pay a bill, you’ve probably used an API.

Today, APIs have become an integral part of both our personal and business worlds. ONC has adopted API certification criteria for electronic health records to help enable access to health information for clinical and patient-facing uses.

How Can APIs Help Patients?

Let’s start with something you’re familiar with. Think about searching for a flight. Before APIs, people had to visit various airlines’ websites to compare prices. Now, there are travel search programs that centralize airline flight information. How do they do this? By using APIs.

APIs in health care are already doing the same things. For example, mobile apps can use APIs to gather data from fitness trackers and add the data to a patient’s personal health record. In the near future, patients may even be able to use an API to electronically share diagnostic information with their doctor in real time - like blood pressure readings, blood sugar levels, and other health information patients generate themselves.

Now that certified electronic health records are required to provide APIs, patients will be able to connect with these APIs to gather and share health information, like from health care providers’ patient portals.

APIs and Health Care Delivery

We’ve seen that APIs can help provide apps with easy and consistent access to health information.

APIs can also help health care professionals improve and simplify care delivery in a number of ways.

First, using APIs, providers can access and use applications and data in electronic health records, or EHRs, in more innovative ways than those available in the existing EHR system.

For example, a pediatrician may be able to use an app specifically designed for pediatric care to automatically perform detailed visualizations and data analysis during regular checkups and provide instant feedback to the parents on the child’s health.

In the future, APIs will make it much easier to share information among health care providers, especially for specific information they may need, such as allowing health care providers to review active medication lists from other EHRs or check a patient’s most recent lab test results.

Real-World Patient API Scenario

Let's take a look at a scenario in which a patient securely accesses her medical records with the help of APIs.

1.) The patient downloads and logs into the app with her username and password.

2.) The patient uses the application to link securely to an API for the health care provider's EHR.

3.) The application sends a request to the patient's health care provider EHR asking for access to her medical records.

4.) The health care provider's EHR validates the request coming through its API and sends back the patient's data to the app.

5.) The patient can now access health information from the app and can merge this information with other health information from other sources - for example, patient portals - to access all the data in one place.

A Closer Look at API Technical Terms

Now that we understand the role that apps and Application Programming Interfaces play for interoperability, let's look at how APIs work.

APIs describe a specific set of technical instructions that allow one piece of software to interact with another piece of software.

When we talk of APIs in health care, most of the APIs work in ways that are very similar to how modern websites work. In general, when an API-enabled app uses the API to make a call from the app to an EHR that has data, the EHR returns data in a compatible cross-application format such as JavaScript Object Notation, known as JSON, or Xtensible Markup Language – XML.

Because the app only needs to know how to call the API, the app can then access data from various EHRs without having to know how the data is stored within each EHR. This makes it easy and quick for applications to combine data and provide new and interesting applications.

APIs in health care typically use a secured version of Hypertext Transfer Protocol, called HTTPS, as the underlying transport technology. Many APIs provide additional levels of security and privacy by using well established industry standards for authentication and authorization, such as OpenID Connect and OAuth 2.0, which are used by some social media platforms such as Facebook and Twitter, to protect a user's identity and their data.

Health IT Security Considerations

We have learned that APIs act as a doorway to data that lets people with the right key get through. APIs work in exactly the same way on different types of devices, in various operating systems, and on a range of mobile devices. When using APIs, remember that the security safeguards required by the ONC certification rule establish a floor of security controls that all certified electronic health records must meet. However, even when using certified health IT resources and tools, there are risks whenever data are shared electronically.

The HIPAA Security Rule can help providers manage these risks. The Security Rule requires providers that are covered by the rule to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic personal health information, or e-PHI. Covered providers are required to perform risk analysis as part of their security management processes. When health care providers add APIs or other new technologies to facilitate information sharing, the best way to identify the risks is to conduct a revised security risk assessment. If the analysis identifies new risks, security measures will need to be put in place to reduce those risks.

This process will help providers protect their practice from threats such as ransom ware, theft, or other types of hacking. ONC offers a Security Risk Assessment Tool online, free of charge, to help small and medium providers assess their risk so they can take the appropriate precautions.

Federal Rules for Data Transfer

There are a number of federal rules that providers might need to comply with when using apps to transmit data.

In 2015, ONC published the Health IT Certification Criteria rule. This regulation requires certified health IT to provide access to health information using APIs.

Under the Health Insurance Portability and Accountability Act of 1996 – or HIPAA, providers must release certain requested data to patients and provide security and privacy technical safeguards. The Office for Civil Rights is responsible for enforcing HIPAA privacy and security rules.

Under Federal Trade Commission rules, health care providers are prohibited from unfair or deceptive acts or practices in or affecting commerce, and they must provide reasonable and appropriate data security.

The Food and Drug Administration requires that apps must protect information accessed or transferred from medical devices.

To learn more about what rules might apply, visit the FTC's portal, which summarizes some of the privacy and security requirements that might apply to Mobile Health apps.

Learning More

To access the tools mentioned in this eLearning module and to learn more, please visit the Resources section of this program.

Thank you.