APIs and the Privacy, Security Challenge for HIM

Save to myBoK

By A. Andrews Dean, CPHIMS, CHDA, CPHI, CPPM, CPC

The Centers for Medicare and Medicaid Services (CMS) turned many healthcare information technology consultants' heads in March 2018 when they announced the new MyHealthEData initiative—intended to continue CMS's goal of digitizing the country's health system and medical records. The initiative came with a hint of emphasis on application program interfaces (APIs) and their transformative role in healthcare to come. While a bold move, many consultants realized this was just the first step toward an API-driven future of healthcare data exchange.

Since then, APIs in healthcare have earned a spot among the many value-based care-related acronyms that have arisen as a result of health IT legislation like the Medicare Access and Children's Health Insurance Reauthorization Act (MACRA). While APIs are just now gaining steam in healthcare, they are more common outside of healthcare. Many people have APIs on their smartphones, frequently just called "apps." There are many types of apps (which have technical differences from APIs but are very similar). The focus in health IT is on the APIs that deal with patient data, an especially sensitive area of data management. APIs are like "apps" that focus on connecting technologies for information sharing and are now set to become the centerpiece and lynchpin of health IT and data exchange in the industry.

Because of this, APIs are going to become a major privacy and security issue for health information management (HIM) this year with the overhaul and continuation of the Promoting Interoperability Program, now combined with two new rules from the Office of the National Coordinator for Health IT (ONC) and CMS on information blocking and implementing the 21st Century Cures Act. These programs and rules promote the use of APIs for exchanging protected health information and put patients in charge of their own data by placing them in the information release driver's seat, requiring payers and health plans to provide access to policyholder data and claims via APIs. Also driving this is that providers are reacting to the government crackdown on information blocking by making their information available via APIs. Taken together, Promoting Interoperability and the new CMS and ONC rules on information blocking and the 21st Century Cures Act are going to cause a real sea change in the field of release of information and HIM. This article will address the many concerns that are related to implementing Fast Healthcare Interoperability Resources (FHIR) and APIs for Promoting Interoperability Compliance (i.e., sensitive diagnoses and treatments, alcohol/substance use/abuse & mental/behavioral issues) due to the absence of privacy and filtering controls in the initial releases of some APIs.

What's with the Emphasis on APIs and Why are They Important?

When the MyHealthEData initiative was announced in March 2018, CMS stated the initiative "is designed to empower patients around a common aim—giving every American control of their medical data. The MyHealthEData Initiative will help to break down the barriers that prevent patients from having electronic access and true control of their own health records from the device or application of their choice."[1] CMS also stated they believed that "the MyHealthEData initiative will work to make clear that patients deserve to not only electronically receive a copy of their entire health record, but also be able to share their data with whomever they want, making the patient the center of the healthcare system."

Then in April 2018, CMS announced the rebranding of "Meaningful Use" to "Promoting Interoperability" effective in 2019 for eligible clinicians and hospitals, which also requires use of the 2015 edition of certified electronic health record (EHR) technology to demonstrate "meaningful use" and qualify for EHR incentive payments, as well as avoid reductions to Medicare payments. The Promoting Interoperability program refocuses EHR use objectives related to healthcare data exchange to encourage care coordination between both patients and providers to promote better patient engagement. The program even includes a measure intended to improve the flow of information via APIs, allowing patients to collect their health data from multiple providers and organize their information in a single program or source. The Promoting Interoperability program requirement to use 2015 certified EHR technology requirements included the ability to provide patients with healthcare data via APIs, which paved the way for APIs to take center stage.

Is Your API a Mobile Medical App? Have You Revised Your Security Risk Assessment Lately?

With more data exchange, the healthcare industry will face even more privacy and security issues. Although the ONC 2015 Certification Rule established a baseline of security controls, risk is always there whenever data is transferred or shared. Although federal rules for data transfer do exist—and the 2015 ONC Certification Criteria Rules require certified health IT to provide access to information using APIs—the burden still exists on health IT vendors, healthcare providers and organizations, covered entities, and business associates to comply with HIPAA.

Under HIPAA, providers must release certain data to patients, and the Office for Civil Rights is tasked with protecting patient data. All healthcare APIs involve healthcare data sharing and must protect data transferred, but not all health IT APIs are technically considered “mobile medical apps,” which are a portion of mobile apps that are subject to additional US Food and Drug Administration regulatory oversight of medical applications.

How can someone know if an API is also considered a “mobile medical app?” Health IT vendors, healthcare providers, plans, and other entities can utilize the Federal Trade Commission’s (FTC) Mobile Health App Interactive Tool, which provides guidance on whether an app or API falls into the special category of “medical device” and determine which federal regulations might apply.[2] Ensuring security and privacy will be an even greater challenge with the increased quantity of data expected to flow between health systems.

Also consider that many APIs’ default settings allow information to flow freely, and in some cases immediately, to the patient when an update is made to the patient chart. Not all APIs may have customizable “release delays” set into them, have robust administrative dashboards for management, or control and filter what information is released to the patient (including such information as substance abuse treatment, mental/physical abuse, or sexual/behavioral health records). Many patient portals have these types of controls, but the healthcare API market is new and not yet mature. Therefore, any APIs used by a healthcare facility should be tested with adequate due diligence, and HIPAA-compliant security risk assessments should also be updated with API usage considerations.

Additional API Information

In late 2018, ONC head Don Rucker gave a brief interview on APIs where he explained their upcoming role in the healthcare industry. The interview is available at https://www.youtube.com/watch?v=jC3j1F0LK80.

To support the implementation of the 2015 EHR certification criteria and meet the requirements of the 21st Century Cures Act, ONC developed an API training module in 2018 aimed at providers and patients who want to understand how APIs work and how they will support access to patient health information and data exchange. This material can be accessed at www.healthit.gov/topic/patient-access-to-medical-records/learning-module-apis-and-health-data-sharing#api-module.

Enter ONC Information Blocking and CMS Interoperability Rules

In February 2019, CMS and ONC announced that Health Level Seven’s FHIR standard would be the required format for APIs—which essentially cemented it as the industry standard for healthcare’s API data exchange platforms—as part of CMS’s and ONC’s proposed new rules on information blocking and interoperability. These rules were intended to further promote and go beyond the MyHealthEData initiative to improve patient access and advance electronic data exchange and care coordination throughout the US healthcare system. The CMS Interoperability and Patient Access Proposed Rule outlined opportunities to make patient data more useful and transferable through open, secure, standardized, and machine-readable formats.

As the new ONC Information Blocking and CMS Interoperability Rules come into play, healthcare provider organizations and health IT vendors will need to be working at a rapid pace to adopt, implement, adapt, deploy, and adjust to newer technologies and information-release protocols. This includes consideration of FHIR-based APIs that are intended to give patients more control of their medical information (and therefore medical history) and review how that information can be shared with other individuals or entities, most of which will fall outside of normal operations for historical record exchange and controls in the healthcare community.[3] It will not be enough for HIM professionals to just change incentive program names and measures and continue doing what they have always done.

What HIM Professionals Need to Know About APIs in 2019 and Beyond

The new emphasis on healthcare data exchange via APIs is expected to have far-reaching consequences, and there is even consideration of re-drafting HIPAA legislation to encourage data exchange and reduce risk. Alternative payment models (APMs) will require population health and more provider-provider and provider-patient data sharing efforts to achieve the APM/accountable care organization goals of cost saving and care improvements. This unfettered data sharing among groups of providers requires more open exchange than HIPAA originally anticipated. The industry is also expected to see a potential shift away, over time, from patient portals as the primary mechanism of data sharing between patients and providers as APIs take the new lead role in this function.

"APIs are the fastest growing business-influencing technology in the IT industry today. The way HIM professionals work and reach consumers/patients is evolving," according to a May 2019 *Journal of AHIMA* article on API governance.[4] "The healthcare industry is seeing a fundamental shift from legacy systems and websites as being the information technology access mechanism for most organizations to the rapidly growing ecosystem of interconnected devices that require APIs to improve business functions."

The use of APIs will not only transform health information exchange and medical records release, but APIs will also contribute in other ways in the research world, such as the Precision Medicine Initiative where programs like "AllOfUs" or "Sync For Science" (S4S) could benefit from pooled data sharing by patients with a health IT API. More information on these programs and how APIs are being used is available at these websites: www.healthit.gov/topic/scientific-initiatives/precision-medicine and www.healthit.gov/buzz-blog/health-innovation/nih-and-onc-launch-the-sync-for-science-pilot. [6]

"API-based approaches to interoperability have the advantage that APIs can be assembled to rapidly create different kinds of aggregate functions," states HealthIT.gov. "However, API-based interoperability still requires attention to important implementation details, similar to traditional interoperability specifications. In particular, given the flexibility of APIs, an API-based approach will need to address many required and optional constraints that are necessary to support a desired use-case."[6]

Within the health IT industry, it may be difficult to find something that has a comparable impact like APIs' on healthcare data exchange practices—how information is shared and transferred will forever be altered in healthcare moving forward.

Also, 2019 Quality Reporting Programs are already underway, and healthcare providers and patients are entering a whole new world of health information exchange. It has taken a long time to get here, but adequate preparation and investment can ensure that everyone achieves interoperability. Organizations that haven't achieved interoperability should further engage with their EHR/health IT vendor, and their app "library" should have all of their available APIs prepared to support information exchange.

This also provides a good time to review an organization's security risk assessments, focusing on any 2015 Certified EHR Technology requirements-related technology changes and API adoptions that may impact an organization's risk profile, technical operations, and performance with government reporting programs. HIM professionals should make sure their organization's IT departments are aware of these API requirements and the need to support them. This will be a truly transformative year for health IT data exchange.

Notes

1. Centers for Medicare and Medicaid Services. "Trump Administration Announces MyHealthEData Initiative to Put Patients at the Center of the US Healthcare System." Press release. March 6, 2018. www.cms.gov/newsroom/press-releases/trump-administration-announces-myhealthedata-initiative-put-patients-center-us-healthcare-system.
2. Federal Trade Commission. "Mobile Health Apps Interactive Tool." April 2016. www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.
3. Centers for Medicare and Medicaid Services. "CMS Advances Interoperability & Patient Access to Health Data through New Proposals." Press release. February 8, 2019. www.cms.gov/newsroom/fact-sheets/cms-advances-

interoperability-patient-access-health-data-through-new-proposals.

4. Primeau, Debi. “Transforming Healthcare Through API Governance.” *Journal of AHIMA* 90, no. 5 (May 2019): 36-37. https://journal.ahima.org/2018/09/01/the-future-of-healthcare-data-exchange/.
5. White, Jon, Josephine Briggs, and Josh Mandel. “NIH and ONC Launch the Sync for Science (S4S) Pilot: Enabling Individual Health Data Access and Donation.” HealthITBuzz Blog. March 21,2016. www.healthit.gov/buzz-blog/health-innovation/nih-and-onc-launch-the-sync-for-science-pilot.
6. Office of the National Coordinator for Health IT. “Understanding Emerging API-Based Standards.” Interoperability Standards Advisory. www.healthit.gov/isa/understanding-emerging-api-based-standards.

A. Andrews Dean (aandrewsdean@gmail.com) is a health IT consultant.

Article citation:
Dean, Andrews A. “APIs and the Privacy, Security Challenge for HIM.” *Journal of AHIMA* 90, no. 7 (Jul-Aug): 18-21.