RHAPSODY

White Paper

How API technology enhances privacy and security and protects patient data

By Shelley Wehmeyer,
director of product marketing, Rhapsody®

Introduction

Our world has never been more connected. Anyone with internet access is now accustomed to immediate, real-time connectivity that brings the world to their computer or smart device. The demand to purchase, post, pin, and pick anything from any website is more pervasive than ever. And it's all made possible by application programming interfaces (APIs).

APIs add value to services and offerings, allowing different devices, applications, and software to communicate and connect to each other. Organizations deploy APIs to enable their customers to make hotel reservations, place orders, track shipping details, and book air travel with ease and efficiency no matter where they are. It is what makes possible all the interconnections people have come to expect and rely on in their daily lives.

At the most basic level, healthcare organizations have been using APIs for a decade—maybe more — whether their IT leaders realized it or not. Single sign-on authentication is a great example of API technology that health IT organizations have adopted and used for years. Modern single sign-on technology is readily embraced and considered a security enhancement. Single sign-on also makes life simpler for clinicians and staff who need to access information quickly.

An API is simply the messenger that takes an individual's request and tells a system what it wants. The API then returns the response back to the individual who made the request.

Two recent events have accelerated wider adoption of APIs in healthcare: government policy and the Covid-19 pandemic. In the United States, the CMS Interoperability and Patient Access Final Rule requires federal payers to make provider directory information publicly available via APIs. Similarly, the ONC Cures Act Final Rule requires health IT certified through the ONC Health IT Certification Program have standardized APIs and implement FHIR standards. CMS and ONC have enforcement mechanisms and penalties for covered entities that do not comply with these rules.

"At the most basic level, healthcare organizations have been using APIs for a decade—maybe more—whether their IT leaders realized it or not."

Covid-19 also ushered in an exponential increase in APIs in healthcare. In 2020, the healthcare industry saw a 400+% increase in API traffic, according to the *State of API Economy 2021*, a report from Google Cloud. The report states:

"Covid-19 is making the increasingly complex need to share data between healthcare providers, payers (insurance companies), and pharmaceutical companies even more crucial. APIs are the key enablers of this data sharing, which is a contributing factor in the impressive API traffic growth within the healthcare industry.

"This API traffic growth in healthcare can be attributed to not only pandemic response efforts, but also the large-scale digital transformation initiatives taking place across the industry. Both patients and professionals now expect and require digital experiences that offer efficiency, accuracy, and privacy, and hospitals and other providers must satisfy this demand to achieve success in 2020 and beyond. Challenges range from providing safe and efficient virtual visits to navigating increasingly complex compliance programs and regulations, all of which can be accomplished through an API-first approach to digital transformation."

Many industries view the use of APIs as beneficial—even instrumental—to how they do business. APIs are used so frequently today because they don't replicate an organization's data, and they don't require a multitude of passwords, which can expose an organization to security breaches and relentless hacking.

While APIs may seem relatively new to health IT, the fact is, this technology is well proven and now is being applied in new ways to make health systems more secure and protective of patient privacy.

This white paper provides insight and answers into the current fear, uncertainty, and doubt that exists among many health IT leaders and addresses:

- The differences between health IT privacy and security in the U.S.
- How APIs have evolved to ensure patient data remains secure as it is used by clinicians and other staff
- How security measures used by API technology and Health Level 7 (HL7) systems compare
- The behavioral aspects of security that come into play when employees share or transport important data
- The advantages of API stateless nature vs. traditional file transfer
- Protecting against API vulnerabilities

Healthcare privacy and security in the U.S. – let’s define the differences

Privacy as a concept is defined as a person’s right to keep his/her individual health information from being disclosed without authorization (HIPAA Privacy Rule, 2003).

Security is defined as the mechanisms in place to protect the privacy of health information. This includes the ability to control access to patient information, as well as to safeguard patient information from unauthorized disclosure, alteration, loss, or destruction (HIPAA Security Rule, 2003).

The American Health Information Management Association defines the Privacy and Security Rules as follows:

The Privacy Rule sets the floor by providing baseline requirements to preserve the overall confidentiality of protected health information (PHI) regardless of type (verbal, paper or electronic). In short, the Privacy Rule:

- Protects individuals’ health records and other identifiable health information
- Protects individuals’ PHI by regulating the circumstances under which an entity may use and disclose PHI
- Requires entities to have contracts or other arrangements in place with business partners that perform functions or services to the covered entity
- Provides individuals with rights with respect to their PHI, including the right to examine and obtain copies of their health records, and to request corrections

The Security Rule applies only to protected health information in electronic form. The Security Rule requires that:

- Covered entities implement administrative, physical, and technical safeguards to protect electronic information
- Covered entities have contracts in place with their business partners that all business partners will appropriately safeguard the electronic protected health information they receive, create, maintain, or transmit on behalf of the covered entities

Why is this important to understand as we discuss API technology? Healthcare entities are legally obligated to manage and protect health information. APIs are a proven solution to manage those obligations with technology that administers access to PHI and how it is transmitted electronically.

APIs ensure patient data is secure as it travels across systems

When designed properly, APIs are not an insecure, open pathway to patient data. APIs have, in fact, evolved and can provide patients with access to their personal medical records. They can simplify the integration between a health system's EHR platform and other data sets—from laboratory information systems to pharmacy records. And APIs connect with EHRs to set the stage for endless possibilities in healthcare information systems.

APIs can provide secure access and break down large data applications hosted on legacy systems. In just a short time span, APIs have dramatically changed how organizations exchange data and, today, are the preferred method for sharing vital data to external parties.

Of course, when health systems use API technology to handle sensitive patient data, access and security controls become a primary focus.

Fortunately, API technology ensures patient data is protected by both managing and enforcing user authorization and authentication. But APIs take security a step further as well.

Through additional layers of security such as dynamic authorization, only the right users get access to patient information. With the use of enhanced access controls driven by policies created by each organization, user permissions are aligned with critical system rules that protect sensitive information and enhance API security.

An added benefit to using APIs is that every request made is an auditable event that can be shown in standard audit log reports for which users or consumers viewed parts of a patient's record. Contrast this with traditional integration methods where flat files of patient records are sent to external organizations. In those configurations, there is no record of who viewed the patient record information or where else that information may have been sent or stored.

"Through additional layers of security such as dynamic authorization, only the right users get access to patient information. "

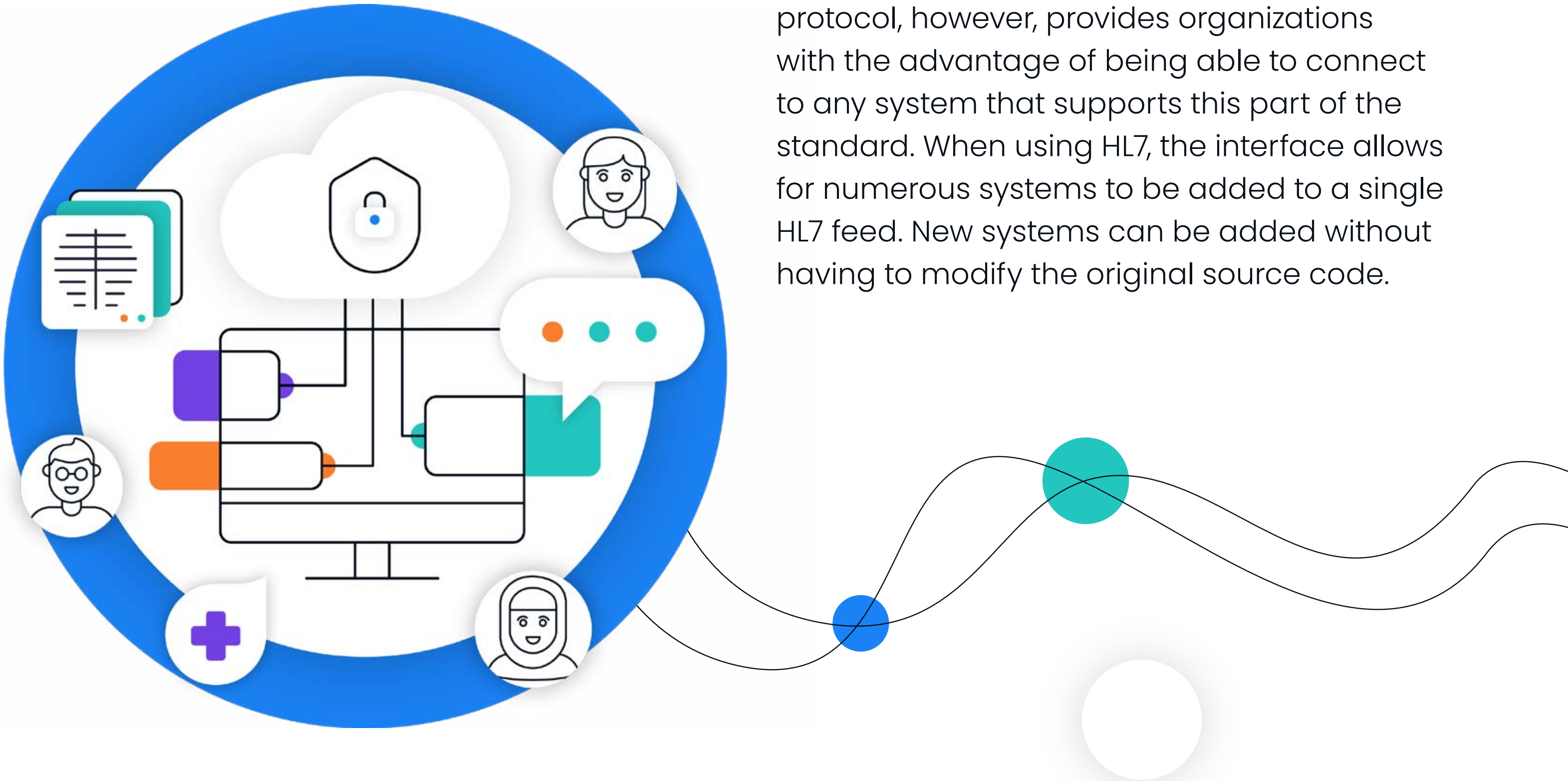
By only exposing key data via APIs, potential vulnerabilities become limited to a small set of endpoints. This approach gives the IT group greater control of who gets access to data with a standard path to authentication. In short, security and other policies are easily applied to this core set of endpoints in a systematic and consistent way. With API technology, an organization can determine its security requirements and apply them uniformly. For example, an organization could efficiently apply multi-factor authentication across the organization with properly implemented APIs in place.

APIs generate auditable events

When third-party applications make requests for patient data, each request is an auditable event. An event is recorded in the source's EHR system, the same way a user logs into an EHR, pulls up a patient's record and views different parts of the record. Because APIs leverage the EHR system for real-time access, the security credentials of each stateless transaction will generate a record that documents who made the request, for which patient, and what data was accessed. Traditional means of sharing records—such as HL7 or flat-file extracts —do not generate the same record of audit capability. Traditional methods of electronically sharing PHI creates undocumented trails of information when they move from one system to another.

Comparing API technology and HL7 systems

API technology is new enough to health IT that we sometimes hear confusion about the advantages of API technology over HL7 platforms.



As we know, HL7 was the first standard protocol for communication between EHR components. HL7 allows for open system architecture, one that interfaces between systems using appropriate protocols, independent of vendor platforms. Following a standard protocol, however, provides organizations with the advantage of being able to connect to any system that supports this part of the standard. When using HL7, the interface allows for numerous systems to be added to a single HL7 feed. New systems can be added without having to modify the original source code.

However, HL7 also presents some challenges. These systems are not plug-and-play. In addition, HL7 implementations differ among vendors. These factors result in incomplete data created by missing fields and values, duplication of data in fields, incompatible data format, and different versions.

Alternatively, API technology operates in real-time collaboration across multiple diverse data sources. For example, blood glucose monitors, EHRs, mobile applications, and wearable activity trackers can all be used to collect and share health data. Through a developer portal, APIs enable users to collect information from multiple data sources and collaborate with each other.

The result: Hospitals can improve workflows, create more patient outcomes, and deliver higher quality of care. Private APIs can be used to bridge the multitude of systems used in hospitals today.

> ***"As the ongoing transition to value-based care, population health management, and care coordination creates an imperative for actionable insights at the point of care, APIs can ensure the electronic health record data is accessible to the right internal and external users while remaining protected from malware and outside threats."***
>
> **Elizabeth O'Dowd**
> Editor of HIT infrastructure

Human behavior factors play a role in privacy and security

In recent decades, new technologies have resulted in new efficiencies and conveniences in nearly every aspect of daily life. This is certainly true in the healthcare industry, where technology has transformed how clinicians and staff communicate and work with each other. Unfortunately, new technology also brings new security and privacy risks—often created by human factors related to the technology available to them.

Study after study shows that organizations have good reason to be worried about employees contributing to cybersecurity risks. Staff may make mistakes that put their company's data or systems at risk —either because they are careless and accidently slip up—or even because they do not have the required training to teach them how to behave appropriately and to protect the business they work for.

Careless or uninformed staff, for example, are the second most likely cause of a serious security breach, behind only malware. In a study by Kaspersky Lab and B2B International, it was found that careless or uninformed staff contributed to 46% of cybersecurity incidents in 2017.

"Many computer security and privacy challenges arise when the expectations of end users do not match the actual security and privacy properties and behaviors of the technologies they use—for example, when installed applications secretly send premium SMS messages or leak a user's location to advertisers, or when invisible trackers observe a user's behavior on the web.

"There are two general approaches to try to mitigate these discrepancies. One involves trying to help users change their mental models about the technologies they use to be more accurate (e.g., to help users think twice before installing suspicious-looking applications), by educating them about the risks and/or by carefully designing the user interfaces (UIs) of app stores. Recent work by Bravo-Lillo and colleagues (2013) on designing security-decision UIs to make them more difficult for users to ignore is a nice example of this approach.

"The alternative is to (re)design technologies themselves so that they better match the security and privacy properties that users intuitively expect, by "maintaining agreement between a system's security state and the user's mental model." Franziska Roesner, University of Washington

User error, or worse, user abuse, is typically the cause of electronic patient records landing in the wrong hands. When first developed, APIs managed security via basic authorization—asking the user for a username and password. This information was then forwarded to the API by the software consuming it, creating a security risk for the organization.

Now, thanks to Open Authorization, an API client can't access user information. Instead, it relays the user to a page on the destination server where he or she must enter username and password credentials. Then the user is returned to the API client where an access token is created.

The benefit of token-based access is that it may be deleted at any time for any reason —a security breach, misuse, expiration, or even if the user decides they no longer want that service to have access to their account. Access tokens can also be used to restrict permissions, letting the user decide what the app should be able to do with their information or account. This process, unique to API technology, reduces the potential for data breaches caused by human error.

Statelessness makes API technology a better system

Health IT leaders understand all too clearly that traditional file transfer tools have not aged well. Common problems include network connections severing in midstream and login timeouts. Further, outdated encryption algorithms are easily compromised, placing data at risk. As organizations strive to continue to secure data and the means by which data is shared, API technology continues to provide critical advantages. One such advantage is the statelessness of APIs.

Statelessness means that every HTTP request made happens in complete isolation. When the client makes an HTTP request, it includes all information necessary for the server to fulfill that request. The server never relies on information from previous requests. If that information is important, the client sends it again in the new request.

The benefit of statelessness is that each request from client to server must contain all the necessary information to understand the request and cannot take advantage of any stored context on the server. What's more, authentication and authorization information is never stored. An access token or client credentials must be provided with each request.

Most IT experts agree that in today's data centers, firewalls and other stateful security controls are less effective than stateless controls or a hybrid approach that combines the two. While stateful security controls are still a necessary part of a comprehensive data center security framework, stateless security controls enhance security and make it easier to manage information without increasing costs.

"Most IT experts agree that in today's data centers, firewalls and other stateful security controls are less effective than stateless controls or a hybrid approach that combines the two."

Protecting against API vulnerabilities

As API traffic in healthcare organizations continues to grow (in many cases exponentially), it is understood that this area of information exchange will be a prevalent cybersecurity target in years to come. With this comes the realization that the creation and management of APIs should approached with security in mind.

Minimizing security threats requires a commitment to and investments in robust API protection strategies. The strategies should encompass security frameworks and governance structures to establish privacy and security workflows, as well as security audits of third-party health apps.

Hiring the right talent, or working with an interoperability partner such as Rhapsody, can help ensure your organization follows best practices for security and privacy, such as:

- Following Open Web Application Security Project (OWASP) Top 10 security concerns for web application security
- Ensuring APIs are up to date on any third-party or open-source dependencies
- Ensuring systems in your organization's infrastructure are running on the latest releases, and quickly deploying fixes if bugs are found
- Ensuring firewalls with rate limiting are in place to prevent distributed denial of service (DDOS) attacks

For further reading, see these resources from HealthIT.gov

Key Privacy and Security Considerations for Healthcare Application Programming Interfaces (APIs)

Accelerating Application Programming Interfaces for Scientific Discovery: App Developer and Data Integrator Perspectives

Summary

Health systems continue to face challenges accessing and sharing data with those who need it to perform their jobs. What's more, as patients become more engaged in their healthcare, they're demanding access to their personal health records. As health IT infrastructure moves to the cloud, and digital information becomes a healthcare industry standard, the concerns for privacy and security will remain a chief priority.

Fortunately, the solution rests with a technology that has proven itself across many industries and has become familiar to each of us in our day-to-day lives. As APIs become points of communication between health information systems, physicians, third parties, and patients, they are developed to ensure patient privacy, secure transfer of data and to simplify interoperability to provide healthcare professionals and users data more efficiently.

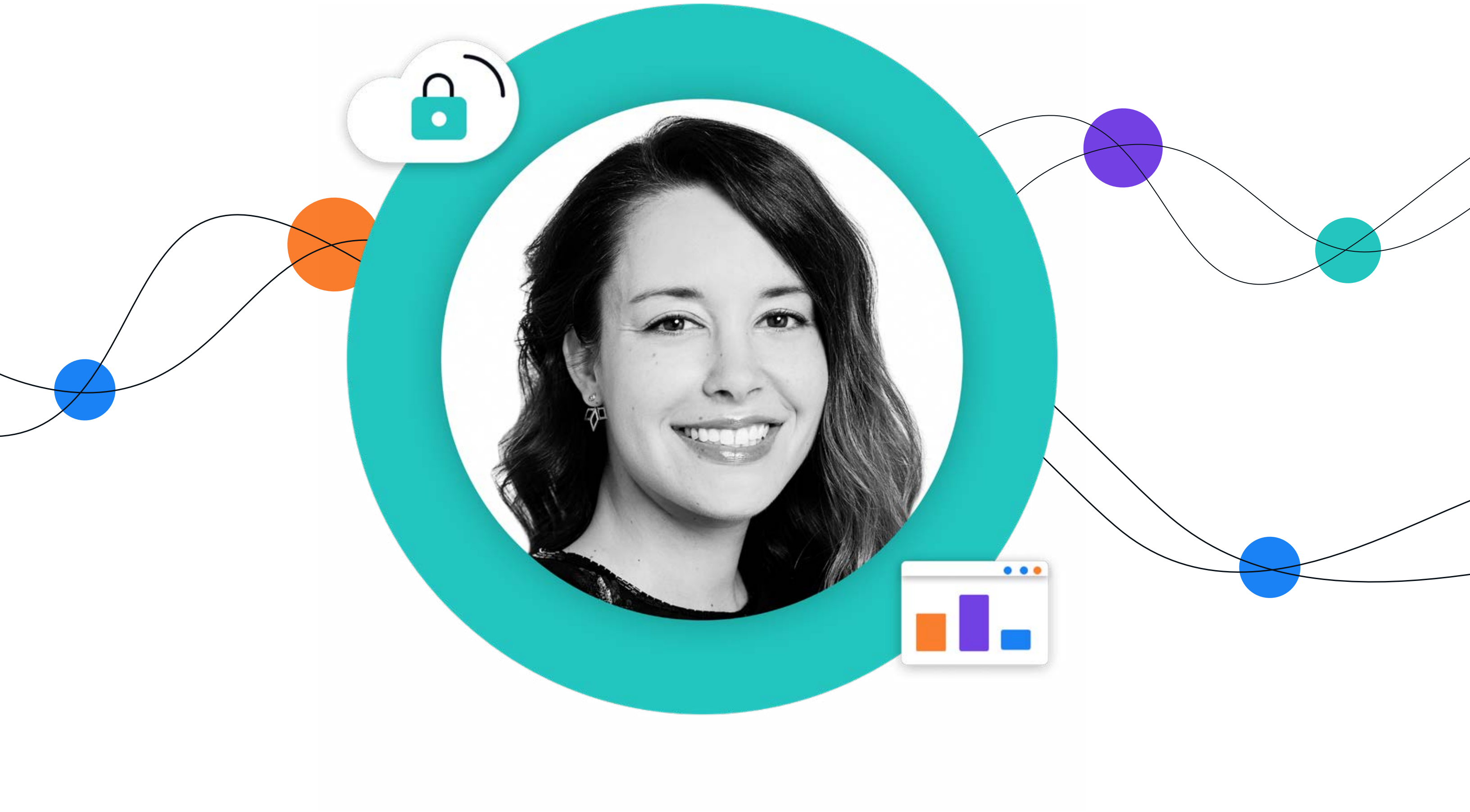
Interested in secure and scalable healthcare API management?

Rhapsody® Integration Engine and Corepoint® Integration Engine give organizations the ability to engage APIs to enable connected healthcare workflows across the business by using web services. Continuous updates make it easier for organizations to work with FHIR and leverage it to its full potential.

Rhapsody® API Gateway works alongside the integration engines to help organizations simplify and secure API management as they ramp up use of API-based data exchange. Rhapsody API Gateway serves as the single API entry point and as a central tool for monitoring API traffic for performance and security—including logging, auditing, and monitoring of availability and access at the API-level.

Learn more about Rhapsody API capabilities.

Get a demo.



About the author

Shelley dedicates her career to simplifying the complexities of health and social care delivery around the world with technology. Whether in the context of navigating the requirements of a new market, launching a new product, or enabling customer-facing teams and customers on product strategy, the most rewarding part of Shelley's experience is the ability to bring together cross-functional, cross-organizational teams to a common goal—doing what is best for the patient and the clinician.

About Rhapsody

Rhapsody partners with healthcare organizations around the globe delivering its adaptable Interoperability Suite to reliably connect, classify, and clean data. Rhapsody health solutions power the applications and workflows that improve clinical, operational, and financial outcomes today while helping teams respond to and prepare for changes on the horizon. Rhapsody is committed to empowering people throughout the healthcare ecosystem, from specialty clinics to large care networks, from public health to health technology, and everything in between.