Navigating the Intersection of Interoperability and API Security in Healthcare

WE ARE AN INDEPENDENT MEMBER OF HLB —
THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

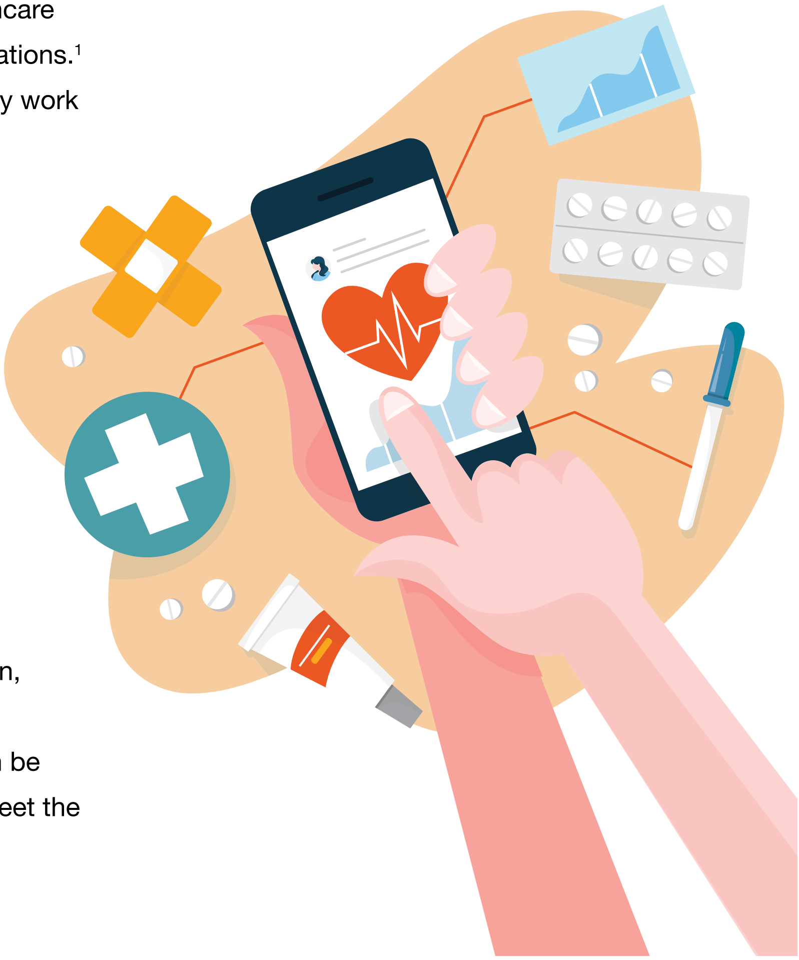
Is your healthcare organization using application programming interfaces (APIs) to aid in interoperability requirements? The answer is most likely "yes," and if so, be aware of these vulnerabilities and risks when implementing APIs.

Interoperability

Health information interoperability is the ability of different information systems, devices, and applications to access, exchange, interpret, and cooperatively use data in a coordinated manner. As of May 1, 2020, it is a requirement by the Centers for Medicare & Medicaid Services (CMS) to aid in provider and patient access to health information. Such interoperability is possible with the implementation of APIs and the use of the Fast Healthcare Interoperability Resources (FHIR) framework.

APIs

APIs are software codes or system protocols that allow different software applications to communicate by facilitating seamless data exchange between healthcare systems, patients, and numerous healthcare applications.[1] In short, APIs are the tools that make interoperability work effectively.



Given the requirement by CMS and the recognized value of interoperability as an enabler of health information-sharing, the use of APIs in healthcare unsurprisingly increased by more than 400% in 2020 and nearly 1000% in 2021.[2] New regulatory requirements are driving providers to establish API connections[3] at this rapid pace. These requirements include the 21st Century Cures Act's focus on data blocking, proposed changes to the HIPAA Privacy Rule establishing an individual's right to transfer data to a personal health application, and the Merit-Based Incentive Payment Program's (MIPS) requirement that patients' health information be accessible through any application configured to meet the technical specifications of an API.[4]

The Rising Threat to API Security in Healthcare

This growth in API usage comes with significant risks that healthcare providers must be prepared to manage. APIs are proving a prime target for cyberattacks, with API attacks increasing by 400% over a recent six-month period.[5]

As the healthcare industry becomes more reliant on APIs to power interoperability, providers are more vulnerable to data breaches due to faulty, vulnerable, or hacked APIs. In 2022, 92% of 397 cloud-native applications—nimble applications that take advantage of the cloud's computing distribution capabilities—experienced at least one API-related security incident, and 57% experienced multiple incidents.[6]

Healthcare data transmitted through APIs contains some of the most sought-after and valuable information, which provides a target-rich environment for cybercriminals. Data breaches can lead to severe consequences, including financial losses, reputational damage, and potential legal ramifications.

Despite this danger, many healthcare providers appear unprepared to manage the risks.

API Vulnerabilities

APIs are vulnerable to standard cyber security attacks, such as distributed denial of service and man-in-the-middle attacks, which can result from the mismanagement of keys and tokens and are due to non-encrypted credentials.

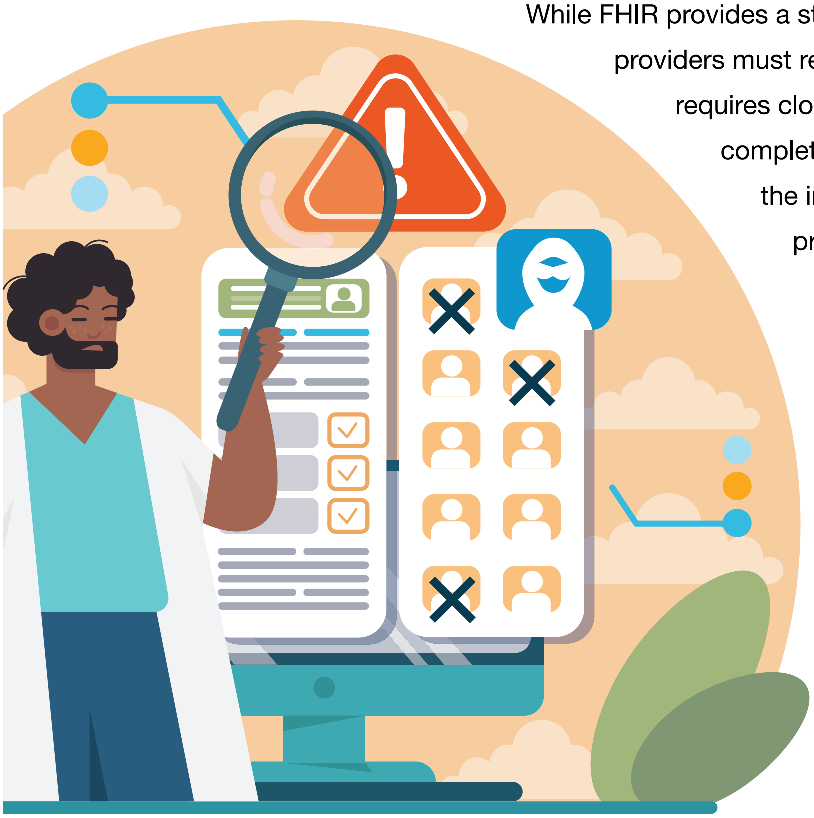
Additionally, a recent joint advisory from the Australian Cyber Security Centre, U.S. Cybersecurity and Infrastructure Security Agency, and U.S. National Security Agency (the "Joint Advisory") highlighted the threat of insecure direct object reference (IDOR) vulnerabilities in web applications, including APIs. These vulnerabilities can allow malicious actors to modify or delete data or access sensitive information by exploiting weaknesses in authentication and authorization. This type of attack is particularly concerning for healthcare organizations that have adopted the FHIR standard for API connections, as these vulnerabilities could potentially be exploited in healthcare settings.[7]

Further, in an FHIR API research study,[8] 53% of the 48 tested mobile apps had hardcoded API keys and tokens that could be exploited to attack electronic health record (EHR) APIs. All tested FHIR APIs allowed access to other patients' health data using one patient's credentials. Specifically, the report discovered a single patient login account could access up to 4 million patient and clinical records.[9]

Another recent study, conducted in 2021, raised concerns about the security of healthcare apps and APIs using FHIR.[10] The study revealed that while EHR vendor implementations of FHIR were generally secure, significant vulnerabilities existed among third-party services, known as aggregators, that gather and compile data and app developers accessing the APIs.

Mitigating Vulnerabilities

With the appropriate implementation of security standards and protocols, threats can be mitigated. The list of known vulnerabilities and resulting breaches illustrate bad actors are aware, ready, and eager to exploit weaknesses. Organizations must take proactive steps to effectively address known vulnerabilities.



While FHIR provides a standard for secure data exchange, health providers must remember the implementation of this standard requires close attention to detail and does not promise complete security. The Joint Advisory underscores the importance of secure implementation to prevent vulnerabilities such as IDOR from being exploited.[11] Healthcare organizations and their security teams must strengthen their security posture by becoming aware of vulnerabilities and being vigilant in the implementation and monitoring of APIs. Bad actors continue to exploit known vulnerabilities, yet the majority can be easily protected. With a thorough understanding of the risks and prioritization of security, the easy exploitation of APIs can be avoided.

Future Trends and Projections

The future of API security in healthcare will be a tapestry woven from technological advancements, regulatory shifts, and an ever-evolving landscape of threats.

Consider, for example, artificial intelligence (AI), which is quickly growing in use. The security of APIs will be impacted both positively and negatively by AI. From a positive perspective, AI can analyze vast amounts of data in near real-time, identifying anomalies in API usage patterns that could indicate a potential security threat.[12] Conversely, AI can also be a dangerous weapon used to exploit APIs. Little doubt exists that cybercriminals will use AI to craft and launch sophisticated attacks, such as reverse-engineering AI endpoints, and the fungible and accessible nature of the outputs from AI in API heightens the risk. These outputs can be manipulated to perform custom tasks and gather responses from the compromised application.[13]

By staying atop trends and proactively addressing potential threats, healthcare organizations give themselves the best chance to ensure they are well-equipped to safeguard their data and uphold their patients' trust.

If you would like assistance with cybersecurity risk mitigation and strategies or any matter involving IT needs, please contact:

Barry Mathis
Principal
bmathis@pyapc.com
(800) 270-9629

Micah Hamilton
Staff Consultant
mhamilton@pyapc.com
(800) 270-9629

As healthcare organizations navigate the intersection of API security and interoperability, they must remain vigilant and reinforce their defenses against potential threats. While APIs in healthcare have provided new opportunities for sharing data and engaging with patients, security threats need to be addressed to protect sensitive information. The Joint Advisory serves as a reminder of the potential vulnerabilities that can be exploited if API connections, including those using the FHIR standard, are not securely implemented. Balancing the regulatory requirements of increased data access and interoperability with the need to protect patient data is a challenging task that requires careful attention to both risk and reward.[14]

How PYA Can Help

PYA specializes in information technology (IT) security assessments and mitigation with our comprehensive risk management Overwatch Program™. We partner with our clients to provide IT risk management, process assessments, and data governance. Our IT subject matter experts have the knowledge and experience to provide professional advisory services, compliance assessments, and audits, and we can assist in IT strategy and integration efforts.

Endnotes

1 HealthITAnalytics. (2022, February 23). Fhir Interoperability Basics: 4 things to know. Retrieved from https://healthitanalytics.com/news/4-basics-to-know-about-the-role-of-fhir-in-interoperability Federal Trade Commission. (2023). Mobile Health App Interactive Tool. Retrieved from https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool

2 Imperva & Marsh McLennan Global Cyber Risk Analytics Center. (2022). Quantifying the Cost of API Insecurity. Imperva. Retrieved from https://www.imperva.com/resources/reports/Imperva-Marsh-McLennan-Report-2022.pdf

3 Alder, S. (2023, May 30). New HIPAA regulations in 2023. HIPAA Journal. https://www.hipaajournal.com/new-hipaa-regulations/

4 Federal Register. (2022). Administrative Simplification: Adoption of Standards for Health Care Attachments Transactions and Electronic Signatures, and Modification to Referral Certification and Authorization Transaction Standard. Retrieved from https://www.federalregister.gov/d/2022-27437/p-3

5 Alder, S. (2023, May 30). New HIPAA regulations in 2023. HIPAA Journal. https://www.hipaajournal.com/new-hipaa-regulations/

6 Keary, T. (2023, May 1). Report shows 92% of orgs experienced an API security incident last year. VentureBeat. https://venturebeat.com/security/report-shows-92-of-orgs-experienced-an-api-security-incident-last-year/

7 Australian Government, et. al. (2023) Preventing Web Application Access Control Abuse. Retrieved from https://www.aha.org/system/files/media/file/2023/08/joint-cybersecurity-advisory-tlp-clear-preventing-web-application-access-control-abuse-7-27-2023.pdf

8 Knight, A. (2021, October 15). Playing with Fhir View. Approov. https://approov.io/for/playing-with-fhir/view/?cid=gyS2dsYYzF

9 Security Boulevard. (2021). FHIR API Security Research Sparks Debate. Retrieved from https://securityboulevard.com/2021/11/fhir-api-security-research-sparks-debate-2/

10 Ibid.

11 Australian Government, et. al. (2023) Preventing Web Application Access Control Abuse. Retrieved from https://www.aha.org/system/files/media/file/2023/08/joint-cybersecurity-advisory-tlp-clear-preventing-web-application-access-control-abuse-7-27-2023.pdf

12 Eliyahu, R. (2022, October 18). Council Post: Three Ways AI Transforms Security. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/10/18/three-ways-ai-transforms-security/?sh=8e8783344983

13 Ibid.

14 Australian Government, et. al. (2023) Preventing Web Application Access Control Abuse. Retrieved from https://www.aha.org/system/files/media/file/2023/08/joint-cybersecurity-advisory-tlp-clear-preventing-web-application-access-control-abuse-7-27-2023.pdf