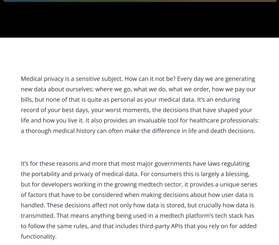
INSIGHTS

Is your API medtech ready?

Adding functionality while maintaining HIPAA compliance

Aug 18, 2023

Andy Heriaud



Medical privacy is a sensitive subject. How can it not be? Every day we are generating new data about ourselves: where we go, what we do, what we order, how we pay our bills, but none of that is quite as personal as your medical data. It's an enduring record of your best days, your worst moments, the decisions that have shaped your life and how you live it. It also provides an invaluable tool for healthcare professionals: a thorough medical history can often make the difference in life and death decisions.

It's for these reasons and more that most major governments have laws regulating the portability and privacy of medical data. For consumers this is largely a blessing, but for developers working in the growing medtech sector, it provides a unique series of factors that have to be considered when making decisions about how user data is handled. These decisions affect not only how data is stored, but crucially how data is transmitted. That means anything being used in a medtech platform's tech stack has to follow the same rules, and that includes third-party APIs that you rely on for added functionality.

Though there are hundreds of regional regulations surrounding medical data, the United States' Health Insurance Portability and Accountability Act of 1996 (also known as HIPAA) provides a great basis for understanding how to choose an API that won't break your platform's compliance.

HIPAA and data

At the center of HIPAA's data protection and privacy rules are electronic protected health information, usually referred to as ePHI. The United States Office of Civil Rights broadly defines ePHI as: "individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form." That means that any identifiers tied directly to medical data must also be treated as ePHI. These identifiers go far beyond the obvious such as name, address, and social security number and include, but aren't limited to:

- Email address
- IP address
- Birth date
- Device identifiers
- Phone number

By law, any company involved in the storing and/or the transmission of ePHI must do the following:

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit.
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information.
3. Protect against reasonably anticipated, impermissible uses or disclosures.
4. Ensure compliance by their workforce.

In the simplest possible terms, users can expect any HIPAA compliant company to require a secure authentication scheme, require regular reauthorization of the authentication scheme, and ensure that all transmitted data, including communications, are 256 bit AES encrypted. It also means that a compliant company has thorough knowledge of where ePHI are stored, whether self-hosted servers, private, hybrid, or public cloud. To satisfy this last requirement, most cloud storage providers offer HIPAA compliant plans where data is stored on bare metal shards in specially designated data centers.

HIPAA requires that any compliant company take proactive steps to ensure compliance throughout their tech stack. This compliance extends to third-party vendors. Any vendor who will handle ePHIs must sign a Business Associate Agreement (or BAA). When you're working with an API vendor, this is where things start to get tricky.

HIPAA's administrative hurdles

Thanks to the widespread adoption of end-to-end encryption, secure multi-factor authentication, and other operational security practices, a large swath of services and platforms would be considered HIPAA compliant on a purely technical basis. But what separates a secure platform from a HIPAA compliant platform is an important administrative aspect. A HIPAA compliant service must sign a Business Associate Agreement (or BAA) with every single other service that they exchange ePHI with. These are bespoke contracts that often come with their own additional stipulations and assurances between the two parties. This can provide an issue at scale that even massive companies take pains to avoid.

Take Google Analytics as an example. Despite being in all likelihood the most utilized analytics platform on the planet, Google makes great pains to clarify that using Google Analytics in conjunction with any ePHI will make your platform out of compliance. The reason isn't technical, it's administrative: Google Analytics is a free platform, and having a team dedicated to drafting, signing, and adhering to a BAA with every single HIPAA compliant customer would be prohibitively time consuming and expensive.

Third-party API vendors face the same logistical hurdles. Consider this hypothetical: you run a HIPAA compliant video chat platform that enables direct video communication between a physician and patient. Your platform is hosted via Microsoft's Azure cloud hosting, and have initiated a BAA via their Product Terms. Your team needs to integrate two features in a short span of time: chat, to enable text communications between patient and physician, and file handling, as many physicians require patients to sign additional paperwork and waivers. Ideally, file handling should be able to be handled via the chat functionality.

Because of cost and time concerns, your team has determined that the best way to deploy these features is through integration with third party APIs. You've identified two companies, one that provides chat and another that provides files, and your team has worked with providers to ensure that the chat and files functionality will not only play well with your platform, but with each other. In order to remain compliant, your company must now sign a BAA with each of the providers.

But that's only half the battle, because now the providers must do the work of each of deploying onto a different tier of their cloud provider that offers HIPAA compliance, and they must each sign a BAA with their providers. Furthermore, since the nature of the integration requires their APIs to communicate with one another, they must also enter into a BAA with each other. Two feature integrations that were designed to be relatively painless have now turned into five different signed contracts.

It's not hard to understand why many third-party API providers refuse to ensure HIPAA compliance, and many of those that do require an enterprise license that is usually tied to an annual contract paid up front to defray costs. But that doesn't mean medtech companies don't have options when it comes to integrating third-party APIs.

Self-hosting and custom cloud deployment

The majority of API providers are actually providing customers with access to their infrastructure. They have developed and deployed hosting environments tailor made to enable the functionality their customers require, and the API provides a simple and secure way to connect the customer's application to their hosting environment. The reason an API provider must sign a BAA is because regulated data has to pass through their servers to operate.

As we've thoroughly discussed, any distinct business entity that is party to the storage or transmission of ePHI is subject to a BAA to remain HIPAA compliant. But what if you could employ a third-party API for functionality, and the API provider was never directly involved in the storage or transmission of ePHI? This is entirely possible, and all it requires is a small amount of engineering work on the part of you and your provider.

Weavy, like a few other API providers, allow developers to bypass our infrastructure entirely if they desire. Our engineers can work with developers who require HIPAA compliance to configure a self-hosted or cloud deployment that keeps all user data within a platform's HIPAA compliant ecosystem. With a self-hosted Weavy environment, ePHI is only ever utilized on your HIPAA compliant server and your cloud service provider who is already covered by a BAA. We can also deploy a Weavy environment on the cloud provider you are already utilizing, meaning data never leaves the HIPAA compliant confines of your provider's data center. With either of these configurations, developers have no need to enter into a complicated BAA with Weavy, as we never have any physical or digital access to user data.

Navigating the regulatory frameworks around medical data is no small task. But a self-hosted or custom cloud deployed API solution like Weavy can enable medtech developers to add functionality quickly, securely, and inexpensively- all minimizing user data exposure and maximizing HIPAA compliance throughout the tech stack.

To learn more about how you can add HIPAA compliant functionality to your medtech platform, reach out to our developer success team here:

Let's talk

Share this post

Read our reviews on G2

Why do developers love Weavy?
Give our reviews a read and find out.

Read reviews >