HIPAA: A Guide for Developers

@MedStack /MedStack info@medstack.co medstack.co

HIPAA is hard for developers. It doesn't have to be.

HIPAA Is Everywhere

HIPAA is the primary U.S. law regulating the privacy and security of health data. It applies to virtually every type of health data: digital, hard-copy, even spoken conversations. Yet for the majority of health app developers, HIPAA is a 'black box', a confusing morass of regulations and requirements that is anything but intuitive. To make matters worse, the majority of information about HIPAA compliance is written for medical providers and clinicians, not app developers.

For health app developers, HIPAA compliance is critical. It can mean the difference between a wildly successful, fully funded new application, and just another new app nobody knows about. Investors want evidence of HIPAA compliance and supporting documentation. Healthcare customers want proof of HIPAA compliance. Hackers will test the strength and resiliency of your compliance as well.

HIPAA Is Hard, but Non-Compliance Is Harder

Failure to comply with HIPAA can result in fines ranging from thousands to millions of dollars. But the loss of credibility and reputation from a data breach can be even worse for app developers, for whom reputation and credibility are paramount. No matter the cost in time and dollars required to comply with HIPAA, the cost of non-compliance is always greater.

Many app developers think they can just ignore HIPAA, or hope it doesn't apply to them. They would be mistaken. HIPAA enforcement has been ramping up over recent years, and in addition to the official HIPAA enforcement agency, the Office for Civil Rights (OCR), recent changes to HIPAA in the HITECH Act gave new HIPAA enforcement powers to each of the fifty U.S. States' Attorneys General. And though it's not officially tasked to enforce HIPAA, the Federal Trade Commission (FTC) has also stepped in to investigate and prosecute technology companies whose claims of data privacy and security are misleading or false.

HIPAA Compliance Actually Is the Answer

HIPAA seems like an enormous burden to many app developers. In fact, HIPAA compliance is one of the best ways for developers to rest assured that their apps and systems are as secure and immune to disaster as they can possibly be. By setting a minimum 'floor' of I.T. security standards based on best practices, HIPAA actually helps protect health data and developers' reputations. By creating data handling procedures that emphasize patient privacy and consumer rights, HIPAA helps ensure customer satisfaction with HIPAA-compliant apps. By requiring specific, written agreements with certain vendors and partners, HIPAA actually clarifies roles, responsibilities and relationships in the app development and deployment supply chain.

Far from being a burden, HIPAA is a well-organized compilation of data privacy and security best practices that app developers in a perfect world should be instituting already, but often don't.

Three HIPAA Mistakes Health App Developers Often Make

There are many ways to fail at HIPAA compliance. For app developers, many of the same HIPAA errors are seen over and over again. Here are three of the most

common HIPAA mistakes developers make and how to avoid them.

Mistake #1 – Thinking HIPAA doesn't apply to your app or your company.
This is perhaps the most common HIPAA error of all. The HIPAA Regulations define certain, specific categories of organizations that are definitely regulated by HIPAA, like medical providers and payers. And technically, all other entities which don't meet the definition are not subject to HIPAA. But in the real world, as well as in our legal system and in the "court of public opinion", HIPAA has now become the de-facto regulatory mechanism for all health data and all entities that handle such data, whether they meet the technical definition of a HIPAA "covered entity" or not. If a breach of health data occurs via an app and patients are harmed (i.e. identity theft), it won't help in court or in the media for the app developer to claim that their system wasn't regulated by HIPAA and didn't need to be configured to HIPAA's security standards.

How to Avoid
If your app receives, transmits, stores or deals with health data in any way, assume that you must be HIPAA compliant. Even if your app only handles anonymized health data, or patient-generated health data, assume that you must become HIPAA compliant, and then become fully compliant.

Mistake #2 – Leaving HIPAA compliance to someone else.
Many app developers and tech companies believe that they can just hire a consultant or expert to "do their HIPAA compliance" for them. This is a misconception. While you may need training, expert help and outside resources to get compliant with HIPAA, you can only be considered "HIPAA Compliant" if you have taken ownership of your entire compliance effort, and can self-certify your compliance efforts via extensive documentation. To be fully compliant with HIPAA, your entire organization must be involved, trained, and familiar with your HIPAA-required policies.

How to Avoid
Make HIPAA compliance a holistic, company-wide effort. To be fully compliant,

everyone in your company, from the CEO to front-line workers, must be part of the compliance effort.

Mistake #3 – Failure to fully document your HIPAA compliance activities.
The best efforts at HIPAA compliance are near worthless if you have not fully documented your compliance activities. Many tech firms and developers have done everything HIPAA compliance requires, but have failed because they couldn't show clear evidence of their compliance. HIPAA compliance requires that a number of specific steps and activities be undertaken, but it also requires clear and complete documentation of compliance activities, so that full compliance can be demonstrated to other parties, like the OCR or a jury in a courtroom.

How to Avoid
Create a clear documentation trail right from the beginning of your compliance efforts. Statements or resolutions from the Founder, CEO or the Board of Directors that commit the company or project to full HIPAA compliance are a huge plus. Memos and emails discussing a commitment to compliance show good faith and clear intent, and are highly valuable. Document everything HIPAA actually requires, but also include materials that show your commitment and intent to be compliant, top to bottom. Imagine you are going to court to prove your HIPAA compliance to a jury. What would you bring and how would you prove your compliance?

HIPAA compliance doesn't have to be complicated.
Talk to us and find out how MedStack can help.

About MedStack

Launched in 2015, MedStack is a cloud automation technology company that builds and manages healthcare privacy compliance into cloud hosting tools. This greatly de-risks application commercialization, and the standardized platform can help bring apps to market 60% faster. MedStack now provides enhanced app hosting and actively managed compliance policies in several countries to over 60 healthcare app vendors in various spaces. The company is proudly based in Toronto, Canada.

@MedStack /MedStack info@medstack.co medstack.co