
# HIPAA COMPLIANCE IN THE CLOUD: FAQS AND MYTHS

Presented by

SINGLEHOP®

# The Cloud Is Viable For HIPAA Applications

To ensure the protection of patient data, the Health Insurance Portability and Accountability Act (HIPAA) lays out guidelines that all companies in the health industry must follow — from primary care providers to data-handling agencies and third-party vendors. HIPAA rules often are complex, however. As a result, some companies inadvertently make mistakes, and others simply remain noncompliant for a variety of other reasons, leaving them subject to penalties that could add up to millions of dollars.

Increases in the use of electronic health records and cloud-based data storage, meanwhile, have made HIPAA compliance even more confusing. Health care providers often are uncertain about whether they're able to leverage cloud resources under this legislation. Adding to the problem are a number of prevalent myths that make it difficult to separate fact from fiction when it comes to health data handling and storage.

The bottom line is that if you operate in the health industry as a covered entity or business associate, HIPAA compliance must be a top priority. Cloud services provide a viable way to store and access HIPAA-protected data, as long as you understand the legislation's basic guidelines. Here's a look at five key FAQs about HIPAA compliance and cloud computing, along with five common myths.

# Table Of Contents


FAQ 1

## What's Covered Under HIPAA?

The short answer: just about everything. Any piece of data that contains personally identifiable information about a patient, any type of treatment plan, or even aggregate data samples that could be traced back to individuals is covered by HIPAA. Your best bet: Assume everything falls under the scope of the law rather than trying to pick and choose.

FAQ 2

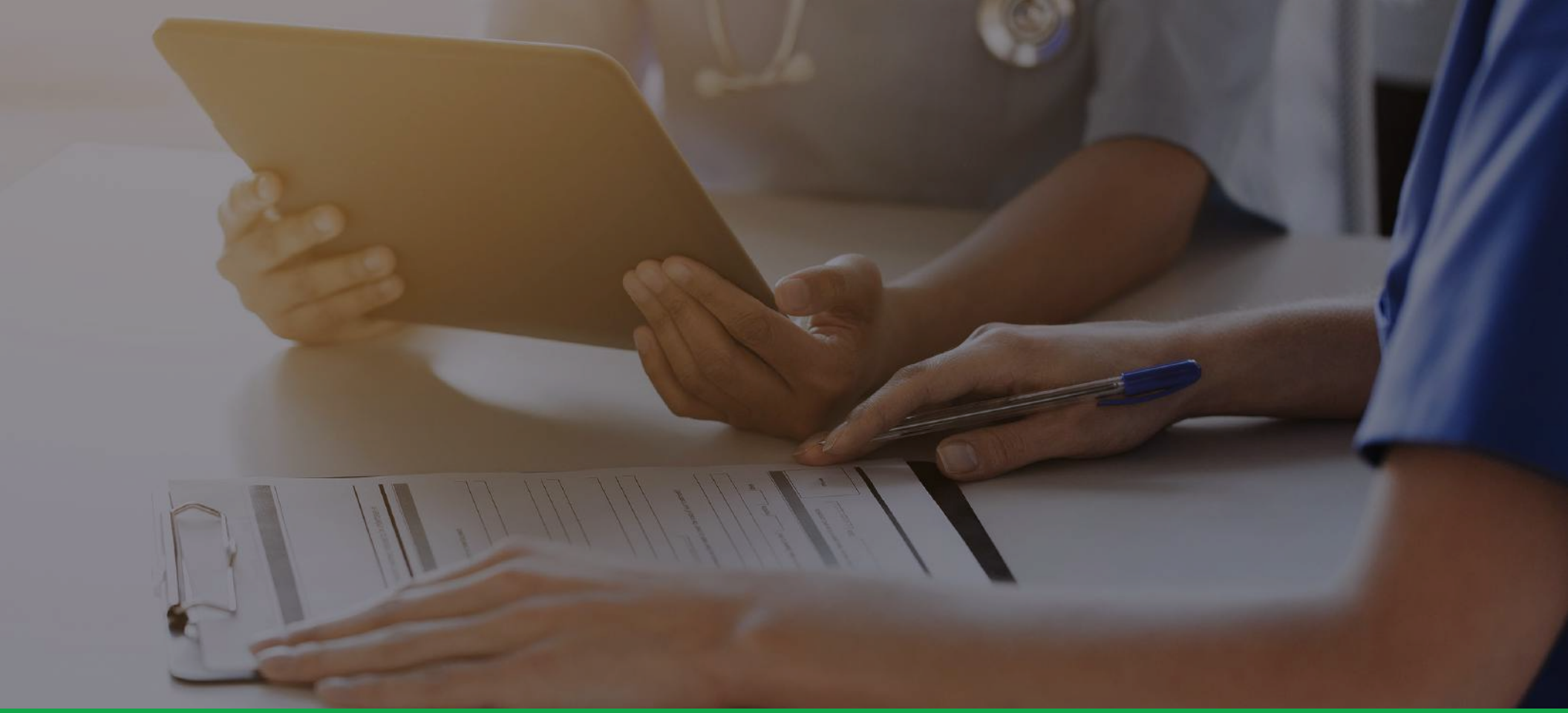
## Is Cloud Storage Acceptable?

Absolutely. There's no requirement for HIPAA data to be stored on-site or handled by a specific agency. In fact, it's not the cloud itself that's the problem when there is a problem — it's how data is transmitted, handled and stored in the cloud that often lands companies in hot water.

FAQ 3

## What's the Difference Between Covered Entities and Business Associates?

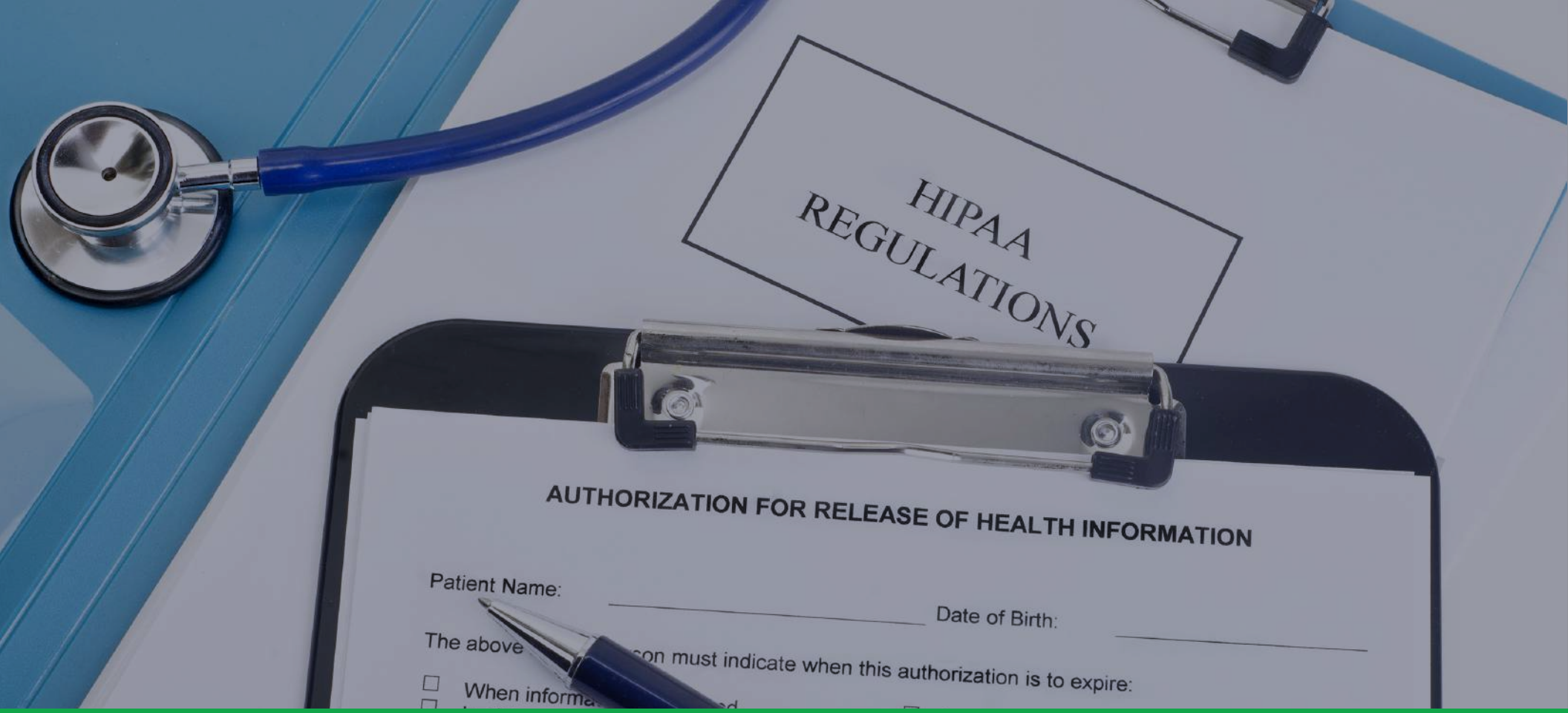
A covered entity is effectively the "owner" of a health record — for example, the primary care facility that first creates a patient profile or enters test results into its electronic health records system. Business associates, meanwhile, include any other company that handles this data. This means that cloud providers, third parties that offer on-site IT services, or other health agencies that access this data all qualify as business associates.



FAQ 4

## Who Is Responsible for Health Data in the Cloud?

Ultimately, the covered entity bears responsibility for HIPAA-compliant handling. While business associates also can come under fire for not properly storing or encrypting data in their care, it's up to the covered entity to ensure they're able to audit the movement, storage and use of their HIPAA data over time.




FAQ 5

# What Does “HIPAA Compliant” Really Mean?

While there is no official “HIPAA compliance” standard or certification that providers can obtain, it’s worth looking for other certifications that indicate good data-handling practices, such as PCI-DSS, SSAE 16, ISO 27001 and FIPS 140.


Myth 1

# Encryption Is All You Need

Encryption is a good start — and should be part of both data transit and storage — but it's not enough. To make sure you're following HIPAA accountability guidelines, make sure you also have a way to remotely lock or wipe devices and track data at any point.

Myth 2

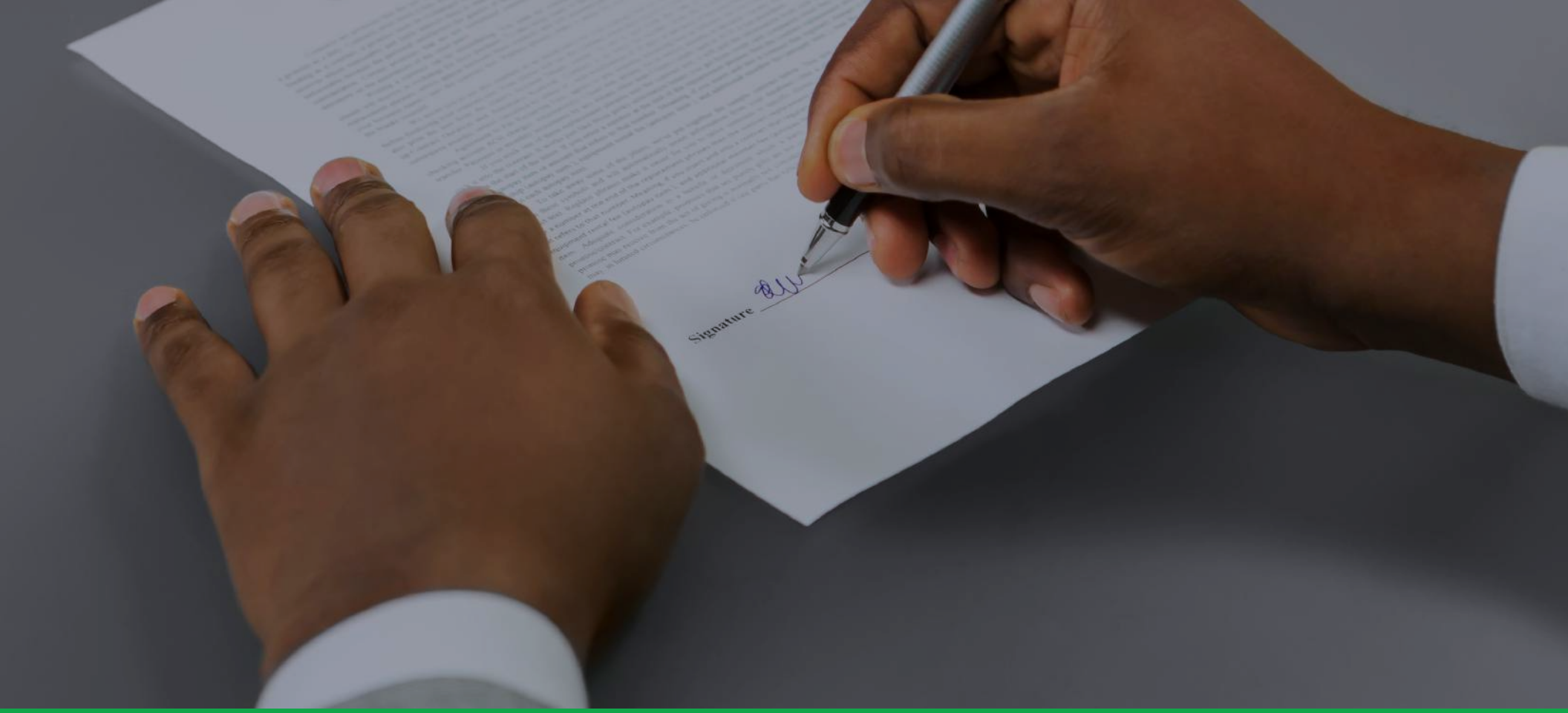
## Cloud Vendors Are The Biggest Problem

In most cases, user error is the issue: Employees accidentally download data they shouldn't or lose devices containing critical information. Staying safe means regular HIPAA training for staff and a cloud provider that offers device-level user permissions based on role and need.


Myth 3

# All Data Service Providers Are Created Equal

As noted earlier, there's no single HIPAA standard for cloud providers, but some are far better than others at keeping health data safe. Best bets? Look at track records rather than marketing materials, and don't let cost drive your decision — you get what you pay for when it comes to protecting health data.




Myth 4

## Business Associate Agreements Aren't for Everyone

False! If you're storing HIPAA data in the cloud, your service provider needs to sign a business associate agreement (BAA). If they're unwilling or reluctant — they'll sign but say it's not really needed or it will make things "more complicated" — take a pass. You're on the hook as a covered entity, and BAAs are an essential part of proving due diligence.


Myth 5

## Once Is Enough For Risk Assessment

To ensure you are using HIPAA-compliant practices, it's a good idea to conduct a third-party assessment. But this isn't a fire-and-forget scenario, especially when you're dealing with cloud providers. Make sure to reassess your risk every year, and include your certified systems professional. An up-to-date risk assessment is well worth the cost if you are randomly selected for a HIPAA-compliance audit by the U.S. Department of Health & Human Services' Office for Civil Rights.

Presented by

SINGLEHOP®

**(866) 349-1027**
or
**(312) 386-6210**
**www.singlehop.com**

SingleHop is a leading provider of hosted private clouds, managed hosting, and Infrastructure-as-a-Service for businesses and enterprises around the world. We bring together a unique combination of enterprise-class technologies from industry-leading vendors and our award-winning proprietary automation engine to deliver a customized infrastructure experience that's available on demand for our customers.