Why You Need a HIPAA-Compliant Chat Provider

Compliance matters. Here's how to protect ePHI as a Covered Entity or Business Associate.

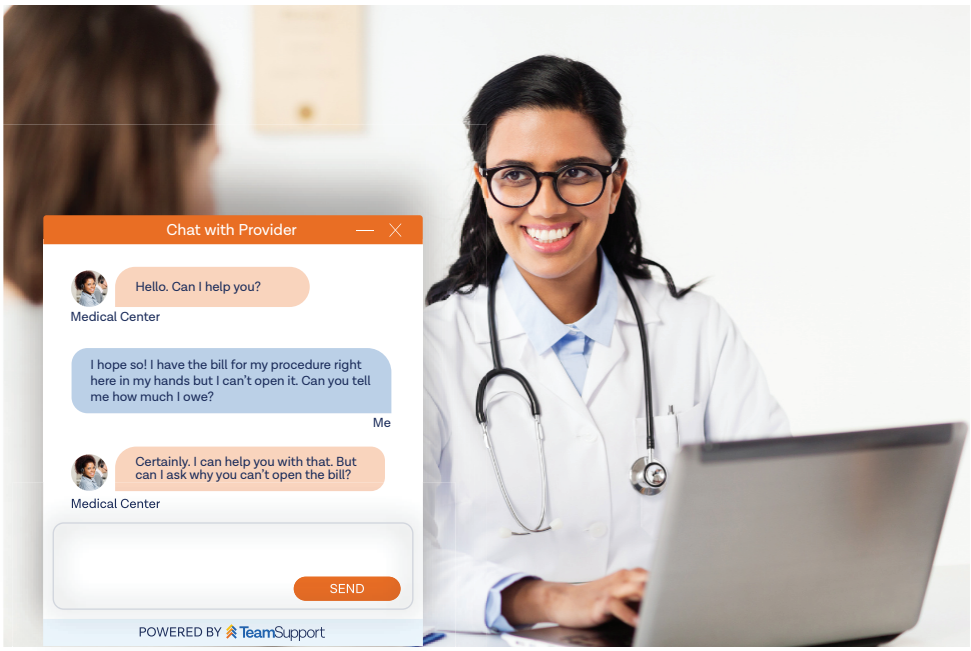
The U.S. Health Insurance Portability and Accountability Act of 1996, (HIPAA) provides a set of instructions and guidelines for the encoding, privacy, security, integrity, and availability of Protected Health Information (PHI). HIPAA encompasses many things, from paper records and electronic transactions to actual conversations.

THE U.S. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

In 2009, the HITECH Act was signed into law and significantly expanded the HIPAA Privacy Rule and Security Rule.

Now, while HIPAA legislation extensively covers all those topics - it lacks an easy to follow checklist when you need to select a service vendor that is HIPAA compliant! How should Covered Entities and Business Associates determine if the messaging provider they're considering meets their organization's security and privacy needs? This guide will provide clarity around what it means to be HIPAA-compliant, how compliance impacts businesses, and the steps your business should take to protect ePHI.

This guide focuses on HIPAA-compliant chat solutions, but many of the policies and guidelines can be applied to other service providers with similar data handling protocols and procedures.



DO I NEED A HIPAA-COMPLIANT CHAT SERVICE?

Even if you're fairly confident that your business requires a HIPAA-compliant chat solution, it's helpful to determine a few things first.

Are you a:

- Covered health care provider (hospitals, clinics, regional health services, individual medical practitioners) that carries out transactions in electronic form
- Healthcare clearinghouse
- Health plan, including: insurers, HMOs, Medicaid, Medicare prescription drug card sponsors, flexible spending accounts, public health authority, in addition to employers, schools or universities that collect, store or transmit EPHI (Electronic Protected Health Information), to enroll employees or students in health plans.

If any of those match, you are a Covered Entity (CE) and HIPAA compliance is important to you! You might even fall into a slightly different category known as a Business Associate (BA) and HIPAA compliance will also apply to you. TeamSupport falls into this category.

BA examples:

- Data transmission providers
- Data processing firms
- Data storage or document shredding companies
- Medical equipment companies
- Consultants hired for audits, coding reviews, etc.
- Electronic health information exchanges
- Medical transcription services
- External auditors or accountants

Lastly but probably most importantly do you handle any Protected Health Information (PHI)?

PHI examples:

- Any conversations a patient has with a physician or nurse about their treatment
- A patient's billing information
- Medical information in the patient's health insurance company's database

If you fit into any of the above categories, we suggest you keep reading.

ORGANIZATIONS MUST TAKE RESPONSIBILITY FOR HIPAA COMPLIANCE

Please keep in mind that even if your organization adopts a HIPAA-compliant technology solution like TeamSupport, this does not "make" the organization HIPAA compliant.

Organizations and businesses must accept the responsibility to ensure HIPAA compliance, and therefore you cannot rely solely on TeamSupport (or any other HIPAA-compliant solution) to make your organization compliant. HIPAA sets forth many policies and procedures that your organization should follow to properly handle and protect the sensitive data you might be collecting. In this case, you want the best HIPAA-compliant chat solution that adheres to those same sets of principles, procedures and best practices. We can partner with you to ensure that your messaging solution is compliant.

ONLY YOU HAVE THE POWER TO BE HIPAA COMPLIANT

KEY POINTS TO CONSIDER

There are a few main points you should keep in mind when evaluating HIPAA-compliant messaging solutions:

Contracts: Get to Know Your BAA

No matter what vendor you might ultimately decide to go with to meet your HIPAA-compliant chat needs, you will absolutely need to enter into a contract known as a Business Associate Agreement (BAA). The BAA is a contract that states your vendor adheres to the same procedures, policies, and obligations to protect and secure your data. There is a good chance you might have multiple BAAs with various vendors depending on what services those vendors or contractors provide.

Tracking AKA Audit Logs

A top of the charts requirement that HIPAA mandates is to keep an audit log of who did what in the service. You need to be able to track who accessed which chat, when they did, and what they did. TeamSupport does provide a full audit log to make sure that you meet this requirement.

Access to Information or “User Roles”

HIPAA specifies that each employee at your organization should only see the “minimum necessary” information to do their job. With TeamSupport you do have the ability to utilize our “Custom Permissions” feature to set up specific access rights for each individual in your organization if you would like. Granted, this requirement is a bit nebulous as to how and what each employee should have access to, but that would be for you to evaluate internally based on the employee role and interactions they might have with clients.

Data Security and Encryption

HIPAA also requires you to secure your data. In the case of using a HIPAA-compliant chat solution your provider must do the same. TeamSupport encrypts data in transit as well as at rest using the most up to data standards such as: 2048-bit keys, TLS, HTTPS, and PFS. TeamSupport makes security a priority to protect our own operations and that same commitment and operational know-how extends to our clients as well.

System Uptime and Backups

HIPAA requires that organizations ensure patient data is available, potentially that data could even be contained in a chat. Naturally this means you need a HIPAA complaint live chat that is stable with good consistent uptime and backs up your data. A great benefit of having this data in the cloud is that even in the event of a disaster at your physical location (assuming you were storing chat records there), and everything was destroyed, you could still retrieve your records.

IN SUMMARY

Protecting sensitive communications should be a top priority for medical providers, insurance providers, and other healthcare-related organizations that handle ePHI. Business Associates and Covered Entities that require a HIPAA-compliant chat solution can rely on TeamSupport to transmit ePHI in situations where speed, privacy, and trust are critical. Contact us to learn more.