

Live Chat & HIPAA

What You Need To Know



Contents

Introduction..... 3

Defining PHI 3

 Couriers & Conduits: Handling PHI 3

 Server-of-Choice: A Good First Step 4

Security and Performance That’s HIPAA-Informed..... 4

 Simplified Data Storage..... 4

 Heightened Login Security 4

 Enterprise-Grade Data Encryption 5

 Sensitive Data Masking 5

 Non-Visitor Specified Reporting Capabilities..... 5

Secure and Flexible Live Chat..... 5



Introduction

If you're discussing health information in your live chat interactions, be sure your platform offers these essential security features to mitigate risk and support compliance.

Handling patients' health information is necessary for many organizations' operations from long-term care facilities and doctor's offices to health insurance providers and managed medical service providers.

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was enacted as federal law to ensure providers and related operations had enough access to information, they need to do their jobs while also protecting the privacy of data related to patients' health. If you are a "covered entity" under HIPAA, you must comply with the limits and conditions on uses and disclosures of protected health information (PHI) and ensure the security of the PHI you handle. But what qualifies as protected health information? And what does this have to do with live chat?



Defining PHI

Protected Health Information (PHI) includes any information about health status, provision of health care, or payment for health care that is created or collected by a covered entity or a covered entity's business associate and can be linked to a specific individual. In most cases, as a covered entity, when you engage with a business

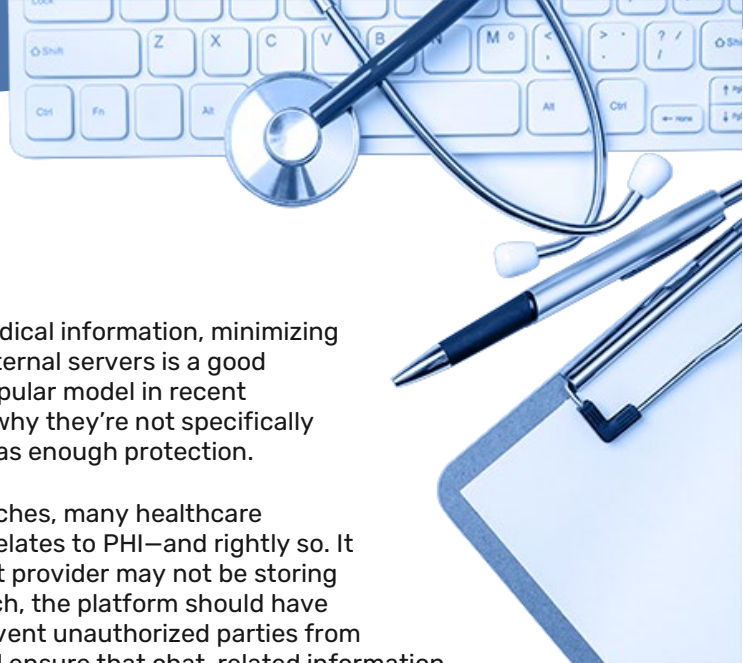
associate to carry out your health care functions, a business associate contract or other arrangement must be made to ensure that the associate complies with HIPAA requirements and is fully audited to protect the privacy and security of PHI. There are exceptions, however, to these auditing requirements.

Couriers & Conduits: Handling PHI

Think of the US Postal Service and private couriers, who may transmit documents containing PHI with a very small probability of exposure. USPS is an example of a "conduit," or an entity that transports information but does not access it other than on a random or infrequent basis as necessary to perform their function or as required by law. Since no disclosure is intended by the covered entity, and the probability of exposure of any particular protected health information to a conduit is very small, the conduit is not considered a business associate under HIPAA.

A live chat provider may also be considered a "conduit" if there are no plans for PHI to be stored on the live chat provider's server. Many live chat providers, therefore, facilitate the storage of chat-related information on a secure server of the client's choice. In this "Server-of-Choice" arrangement, live chat software providers simply act as "conduits" of the data that is being transmitted over their platforms.

“ In a "Server-of-Choice" arrangement, live chat software providers act as "conduits" of the data that is being transmitted over their platforms.



Server-of-Choice: A Good First Step

For companies working in health care industries or with medical information, minimizing risk by avoiding the storage of protected health data on external servers is a good first step. Server-of-choice has become an increasingly popular model in recent years and plenty of live chat providers have written about why they're not specifically HIPAA compliant, pointing to the conduit treatment of PHI as enough protection.

However, given the recent number of healthcare data breaches, many healthcare organizations are concerned about live chat security as it relates to PHI—and rightly so. It is important to bear in mind that even though your live chat provider may not be storing protected health information, they're still handling it. As such, the platform should have safeguards that prevent unauthorized parties from intercepting PHI and ensure that chat-related information and transcripts are archived properly.

“ Even though your live chat provider may not be storing protected health information, they're still handling it. The platform should have safeguards that prevent unauthorized parties from intercepting PHI and that ensure chat-related information and transcripts are archived in a proper manner.

Security and Performance That's HIPAA-Informed

Leading live chat platforms provide a heightened level of security through a comprehensive set of features that begins with server-of-choice and should include these five safeguards:

Simplified Data Storage

As we've established, your live chat provider should enable your organization to fulfill HIPAA compliance by facilitating the storage of your chat information on a trusted server of your choice. The key, however, is making it as easy and painless as possible.

Heightened Login Security

Your login screen is, in many ways, the gatekeeper of your live chat platform. The processes that power this interface are critical to keeping protected health information out of the wrong hands. Inquire about your live chat provider's password management options, including character requirements and password expiration.

Two-factor authentication is also an option to look for. Often employed by systems where sensitive information is being managed, this feature requires the user to pass two checkpoints to gain access. In banking, this means having the debit card in hand and also entering a PIN number. In live chat, it might mean entering a password and selecting a personal security image or answering a security question. IP-based login restrictions are also available through some live chat systems to provide an added layer of access control.

Enterprise-Grade Data Encryption

When you're handling sensitive customer information, and potentially protected health information, keeping your data secure must be your top priority. Look for live chat platforms that encrypt all chats and transactions recorded within the system using 256-bit SSL (secure socket layer) standards. Ask about firewalls, intrusion detection systems, application content filters, anti-virus software other mechanisms that prevent unauthorized access and defend against the injection of malicious and potentially harmful content.

“ If your chat information is not being stored on the platform's server, it's important to ask how this will impact the platform's ability to monitor your performance.

Sensitive Data Masking

Sensitive data masking, a feature offered by industry-leading live chat platforms, prevents sensitive information, like a credit card number, from being viewed by replacing the appropriate text with X's. Typically, this is offered as an option both within a live chat interaction and within the chat archive, allowing you to minimize exposure of private information both during and after the chat session. Additional options, such as disabling copy and paste within the live chat platform, can also help reduce the risk of sensitive information being distributed.

Non-Visitor Specified Reporting Capabilities

Many live chat platforms tout robust reporting capabilities; however, if your chat information is not being stored on the platform's server, it's important to ask how this will impact the platform's ability to monitor your performance. Look for a live chat software that can track valuable metrics related to agent utilization, service level performance, and customer satisfaction even when your chat transcripts are stored elsewhere.

Secure and Flexible Live Chat

Live chat has become a mainstream asset for savvy businesses across industries – and health care is no exception. However, if you handle health information and are a covered entity under HIPAA, compliance should prompt some additional considerations as you vet live chat platforms. Do your homework and ask the right questions. By choosing an experienced and flexible live chat partner, you'll ensure the security of your interactions without sacrificing the features that make live chat such a valuable tool for both your customers and your organization.

Chat with us at [velaro.com](https://www.velaro.com)

