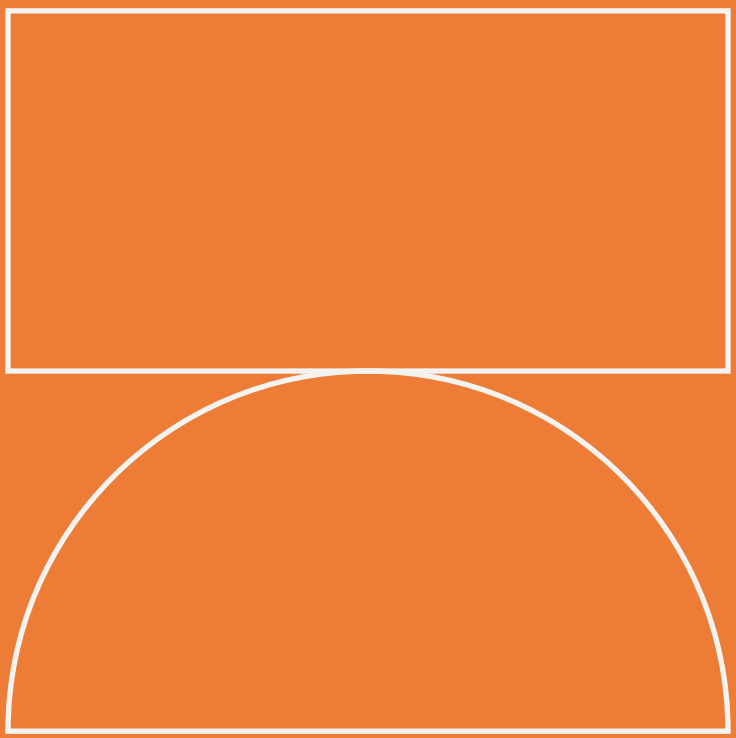
Healthcare guide to HIPAA compliant messaging



sendbird

eBook

Table of contents

Introduction

Research increasingly shows that patient satisfaction is strongly linked to communication between healthcare providers and their patients. In fact, a 2016 study found that effective communication from providers was the strongest predictor of high patient satisfaction. With the rise of value-based care, patient-centered communication, healthcare concierges like Accolade, and advances in healthcare technology, results-focused healthcare providers are ensuring that the patient experience remains at the center of every strategy and new technology.

An elevated patient experience requires the same seamless mobile communication that people are used to throughout their daily lives. And mobile healthcare communication is in high demand. A global study conducted by FICO found that 80% of people would like to use their mobile phones to interact with healthcare providers.

Doctors, nurses and administrators also see the clear benefits of asynchronous communication from their smartphones:
It's easy, convenient and effective. But for healthcare organizations to give both patients and providers the communication channel they want, they need a messaging and chat solution that is both easy to use and HIPAA compliant.

The challenge: choosing a HIPAA compliant communication channel

Needless to say, any electronic patient communication must be HIPAA compliant. This requirement can pose a significant challenge to healthcare organizations because most patient communication solutions are provided by third-party vendors.

The risks of non-compliance are very real. In a study published by the Journal of the American Medical Association , researchers attributed only 6.2% of Protected Health Information (PHI) breaches to hacking IT incidents by undisclosed entities, while they attributed an astounding 53% of PHI breaches to the internal staff of healthcare entities. Of the breaches, 46.1% originated on mobile devices. Among the 20% of breaches occurring during PHI communication, 34.5% occurred during email interactions, underscoring the risk of e-mail.

It's a lot of numbers, but the big takeaway is this: If your internal staff communicates with patients electronically, then they must do so within the guidelines stipulated by HIPAA and HITECH.

Therefore, it's essential that your healthcare organization finds a communication solution that is already HIPAA compliant to prevent these PHI breaches before they occur. It's the most effective way to prevent your staff from breaching PHI.

Why your HIPAA-compliant messaging solution should sign a business associate agreement (BAA)

No guide to HIPAA-compliant patient communication should exclude this advice: All covered entities should enter into a BAA with their business associates and should not do business with patient communication providers unwilling to sign a BAA.

The HIPAA Security Rule establishes a set of security standards for protecting electronic protected health information (ePHI), and it applies to 'covered entities' like health plans, healthcare clearinghouses, and any health care provider who transmits ePHI during internal operations or with their business associates. Basically, it requires covered entities to maintain administrative, technical, and physical safeguards for protecting ePHI.

There are four general mandates:

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; and
4. Ensure compliance by their workforce.

Fines for breaches can be steep—up to $1.5 million for eachidentifiedbreach — and some breaches can be criminally charged.

HITECH requires technology partners to assume the same liability as healthcare entities

Prior to the HITECH Act of 2009, HIPAA was not explicit about the liability of technology and healthcare solution providers. After passing, however, the act required that technology and healthcare solutions providers assume liability for the Privacy and Security Rules.

The HITECH Act of 2009 calls these solutions providers "Business Associates," or anyone transmitting or receiving PHI. And it holds them directly accountable for HIPAA violations, requiring them to create physical, technical, administrative and organizational frameworks for protecting PHI.

Under HIPAA and HITECH, in other words, both "covered entities" and "business associates" share responsibility for protecting PHI and both enter into a "business associate's agreement" (BAA) to commit legally to that responsibility.

In effect, the commitment to uphold the HIPAA Privacy and Security rules is an agreement by both the covered entity and its business associates and solutions providers. If a healthcare communication solution you're considering working with refuses to sign or avoids a BAA, then that signals a lack of confidence that it can maintain compliance with HIPAA. And that's a dealbreaker.

Patient-and mobile-friendly communication

Now that you're familiar with the HIPAA Security Rule, the HITECH Act of 2009, and the importance of an agreement between your business and its associates, it's time to understand how your healthcare company can engage in effective mobile communication with patients.

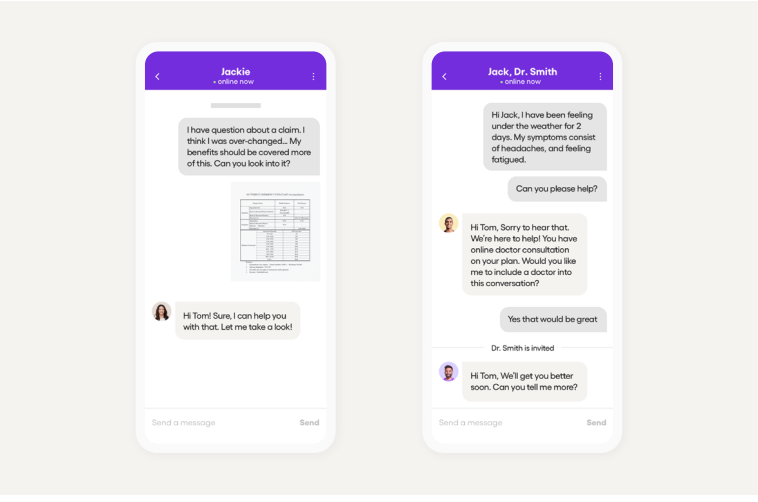
When healthcare companies consider a digital or mobile communication strategy, three channels tend to dominate the conversation: in-app chat, SMS, and email.

HIPAA compliant in-app chat: the most secure patient communication

In-app chat is a global phenomenon. There are more than 5.8 billion users of messaging apps in the world—roughly 76% of the global population. Many API and software as a service (SaaS) companies provide a chat platform for healthcare

companies to integrate chat into their applications. As with other patient communication solutions, the key is to find chat providers that are HIPAA and HITECH compliant — plus willing to sign a BAA.

Many healthcare in-app chat providers control the full technology stack behind their technology. As a result, there's no interoperability with third-party systems that could pose compliance risks. As we'll see in the HIPAA-compliant email section below, this is just one of the many benefits of in-app chat.



In-app chat can be one of the most secure ways to conduct HIPAA-compliant patient communication because:

- Log-in requires user authentication
- Each user has a unique ID
- Chats and data are encrypted in transit using TLS/SSL and at rest using AES256
- Many companies will keep continuous logs, making audits possible
- Retention of chat messages and other data can match your organizational policy
- Chat solutions provide secure photo, video, and other file sharing
- You can set how long a message will persist in the application
- Read receipts acknowledge whether a patient or healthcare provider has read a message

Risks associated with in-app chat:

- Some chat providers claim they are HIPAA compliant, but they do not sign a BAA
- It is imperative that you do not disclose any ePHI in push notifications that link back to in-app chat. Instead, notify the user of their in-app chat with a message like, "You have a new secure message,"

accompanied by a link that requires authentication.

HIPAA-compliant SMS: balancing risks with benefits

Although SMS (i.e., texting) is a 20-year-old technology, it's still the standard for mobile communication. Everyone has a phone in their pocket, and some studies estimate that 90% of texts are eventually read. Even though these conversations tend to be one-way, healthcare companies can still communicate valuable information in simple exchanges.

The key challenge of SMS, however, is security and HIPAA compliance. Generally speaking, SMS is not HIPAA compliant because it is not an encrypted channel.

If you are looking for HIPAA-compliant SMS, you must find solutions that can meet the following requirements:

1. Under HIPAA's Security Rule, every authorized user must have a unique ID and password for an SMS solution, so communications can be monitored and logged
2. Your SMS solution must have automatic log-off, so unauthorized users cannot access ePHI if they gain access to the phone

3. Your SMS solution must encrypt the communications in transit so they cannot be intercepted at any time, and any PHI must not be readable or usable

Because SMS uses telephony networks and sends messages directly to phones, it's difficult for SMS solutions to meet these three criteria. SMS solutions will therefore require an additional thirdparty security integration — and add an extra layer of complexity.

Other risks associated with SMS

- Text messages may stay on a mobile device indefinitely, exposing ePHI to unauthorized individuals after theft, loss, or recycling of the device
- Text messages do not require authentication, so users with access to the phone have access to its text messages without a password
- Texts are not typically subject to an administrator or monitor, so access cannot be easily logged or audited
- While text messages are usually encrypted by the carrier, the encryption standards are not as high as information communicated over-the-top, which uses TLS, SSL, or AE256
- The HIPAA Privacy Rule gives individuals the right to access or amend their PHI.This is difficult to do with text messaging technology, especially when the information is distributed across the patient and healthcare provider's phone

CPaaS as a "conduit"

Some communications-platform-as-a-service (CPaaS) companies now argue that they are no longer "business associates" and merely "conduits"

under the rules of HHS. Following this legal claim, they suggest that they will not sign BAAs because they are exempt from any liability pertaining to breaches of ePHI.

Even if you accept this legal argument, using SMS as a patient communication channel can expose your internal staff to greater risk of ePHI breaches because the physical device is not secure. Remember — internal staff comprise 53% of ePHI breaches. Therefore sole responsibility rests on the shoulders of your healthcare organization, the covered entity, and exposes you to greater risk.

HIPAA-compliant email: implementing safeguards beyond encryption

Email is also a tried-and-true method of mobile communication, but lacks the advantage of real-time communication and consistent encryption.

Email always prioritizes deliverability over encryption. This has an important consequence: even if the sender's email client supports encryption, it will send the email without encryption if the recipient's email client doesn't support encryption. Email providers would rather send the email than guarantee encryption. Even when an email has been delivered with encryption, it doesn't necessarily mean that patients will open it. Studies show that about 25% of email remains unopened after 48 hours, compromising the efficacy of your communication.

Compliance on e-mail varies from provider to provider. Although many of the popular consumer email providers (including Gmail) provide encryption, they are still not an adequate HIPAAcompliant communication solution because, in practice, they must support interoperability with a

broad range of legacy mail servers that don't support TLS encryption.

If you are looking for a HIPAA-compliant email solution, you must find solutions that can meet the following requirements:

1. Encrypt email 100% of the time from sender to recipient.
2. Support automatic log-off, so unauthorized users cannot access ePHI if they gain access to the phone.
3. Retain messages for up to six years, so you can monitor and log any ePHI communication and users can modify, delete, or access their ePHI at any time.

Because email encryption depends on both the sender's and recipient's email clients' supporting it, encryption is anything but guaranteed. If a sender's client supports encryption and a reader's client does not, then the email is transmitted in plain text and becomes an ePHI breach.

That said, HIPAA-compliant email solutions do exist and should be checked for the criteria above. However, email may not be the best choice for a mobile communication strategy.

Patient-centered communication

Whether you choose an in-app chat provider or choose to manage risk with SMS or email, it is important that doctors, nurses, and support staff communicate well to create a great experience for patients. There's a lot of research that discusses how good communication can improve patient satisfaction and even a patient's health outcome. In this section, we summarize some of the research to help you establish guidelines for how you communicate with patients once you've selected a digital communication channel.

Research on physician-to-patient communication has suggested and endorsed a model of "patient-centered communication," to improve patient-experience during important conversations about a patient's health. As with in-person communication, digital communication between patients and their healthcare providers could benefit from making patient-centered communication an internal standard.

In two studies that asked patients about ideal physician behavior, researchers concluded that patients prefer patient-centered communication. We suggest that your business incorporate this research into your communication training and guidelines for physicians and other support staff.

According to the research, patients said they want their physicians to[1]:

[1]Source: Ann King, Ruth B. Hoppe. "Best Practice" for Patient-Centered Communication: A Narrative Review." J Grad Med Educ. 2013 Sep; 5(3): 385–393)

1. Explore the patient's ideas about a health problem — their thoughts, worries, feelings, expectations — and take the patient's input seriously
2. Understand the whole person and deeper context like family influences or how the problem might affect the patient's life (i.e., recognize that a person's biomedical diagnosis does not define them)
3. Tell the patient what is wrong in plain language
4. Seek common ground and partnership. Agree on the nature of the problem, the priorities, and the goals of treatment; make management decisions and clarify the respective roles of the physician and patient
5. Strive for an enhanced physician-patient relationship. Be approachable and friendly, share decision making, show genuine care, and be respectful

When you can integrate these themes into your patient communication strategy, you'll provide patients with patient-centered communication that drives higher patient satisfaction.

Other standards for your patient-centered communication strategy could include:

1. Be uncomplicated
2. Be specific
3. Use some repetition
4. Minimize jargon
5. Check patient understanding

Recent studies have shown that effective communication is associated with better patient outcomes like "physiologic measures (e.g., blood

pressure, blood glucose levels), health status (e.g., headache frequency, depression), and measures of functional status, including less patient distress with the illness experiences."[1]

Using patient-centered communication as a model can help your business establish communication guidelines across your digital communication solutions and staff. Combined with HIPAA-compliant patient communication, the patient-centered model will meet patients wherever and whenever they need and provide even more convenient and effective healthcare.

[1]Source: Ann King, Ruth B. Hoppe. "Best Practice" for Patient-Centered Communication: A Narrative Review." J Grad Med Educ. 2013 Sep; 5(3): 385-393)

HIPAA-compliant in-app chat: secure way to message patient

Effective communication from healthcare providers is the best predictor for high patient satisfaction and, increasingly, both patients and healthcare providers recognize that mobile communication is the most convenient way to give patients access to healthcare anytime, anywhere. For healthcare entities beginning their mobile communication strategy, or even changing it, maintaining HIPAA compliance is the greatest challenge. In-app chat is by far the most secure channel for mobile communication, but, no matter your solution, ensure that your solution provider is willing to sign a BAA, so you can have confidence as you pursue your new patient-centered communication channel.

Explore Sendbird's HIPAA-compliant in-app chat solution or set up a consultation with one of our healthcare experts.

Get started


sendbird