spruce

Using Spruce in a HIPAA-Compliant Way

Executive Summary

We built Spruce for healthcare. We wanted to make it easy and safe for providers to communicate with their patients in a wide variety of ways — calls, voicemail, text, in-app message, fax, video — all from one tool. With that in mind, we developed the Spruce platform to ensure three fundamental tenets:

- That Spruce's underlying technologies are compatible with the security and privacy requirements in place to protect and secure protected health information (PHI) under HIPAA;
- That Spruce operates based on policies and procedures that let us meet and exceed the obligations of a business associate under HIPAA, including all necessary administrative, technical, and physical safeguards; and
- That providers on Spruce can use each of our platform's supported communication channels in a HIPAA-compliant way, as part of a HIPAA-compliant practice.

Every communication channel is different. Some channels, such as in-app messaging and videoconferencing, are inherently secure and encrypted. Other channels, however, depend on older technologies that neither Spruce nor any other service provider can control or secure completely, such as SMS texting. This often means that such channels cannot independently meet the demands for technical safeguards that are present in HIPAA. Despite this limitation, **there are still easy ways to remain HIPAA-compliant while using all of the communication channels supported on Spruce.**

In this document, we'll provide you with a guide to help you evaluate your practice's approach to patient and team communication under HIPAA and show you how you can most effectively and safely use Spruce.

While we encourage you to read this entire guide, the table below provides a brief overview of each communication channel supported by Spruce and what you need to do to use it in a HIPAA-compliant manner.

Table 1:
HIPAA Compliance and Communication Channels

Channel	Underlying Technology is HIPAA-ready	Patient Consent Required
	Channel either (a) meets the necessary technical requirements of HIPAA or (b) has a specific exemption under HIPAA. Basic HIPAA practices still required (e.g., minimum necessary PHI, verifying patient identity before sharing PHI, etc.)	Channel is not inherently secure but can be used with informed patient preference. Basic HIPAA practices still required (e.g., minimum necessary PHI, verifying patient identity before sharing PHI, etc.)
Secure App-to-App Messaging	✓	
SMS Text Messaging		✓ *
Video Calls	✓	
Spruce Visits	✓	
Phone Calls	✓	
Voicemail and Transcription	✓	
Email		✓ *
eFax	✓	

*The federal government has advised that patients have a right to receive health information via their preferred communication channels, including unencrypted channels, should they prefer them. It is important to understand patient communication preferences, as they may be both protective and mandatory.

Table of Contents

Business Associate Agreements

The first and most important step toward using Spruce in a HIPAA-compliant manner is establishing a business associate agreement (BAA) with us. We're also happy to say that a full-force BAA is included automatically in the standard Spruce terms of service for organizations, provided that your organization is subject to HIPAA.

To a close degree of approximation, HIPAA considers any outside person or company that interacts with an organization's PHI to be its business associate, and this means that many users of Spruce will need a BAA with us in order to satisfy their obligations under HIPAA while using our platform. This BAA doesn't change anything in the technology that we provide you, but it is a requirement under the law to stay compliant with HIPAA.

Bottom Line:

You need a BAA with your communications provider (Spruce) in order to be HIPAA-compliant, and a compliant BAA is included automatically in the standard Spruce terms of service for organizations.

Communication Channels

Messaging

There are two ways to message with patients on Spruce: secure (app-to-app) messaging and traditional SMS text messaging. We'll break each type down below.

Secure Messaging

You can message securely with your patients if they have downloaded the Spruce app. We recommend that providers encourage their patients to download the app to communicate in this way.

On Spruce, if you start a secure messaging thread with a patient (denoted by a lock icon on the thread), you can be assured that all communication between you and the patient is occurring within the Spruce application, which includes HIPAA-grade encryption and other controls for all information exchanged, both when the information is stored and when it's being transmitted. This also applies to all conversations that you have on Spruce with your teammates, and it makes your job under HIPAA much easier.

As always, you need to ensure that you're following basic HIPAA principles, such as verifying patient identities and sharing PHI only with necessary teammates, but the technical safeguards present within the Spruce system ensure that the heavy lifting is already done for you. You can use secure messaging and team conversations on Spruce for all typical medical uses under HIPAA.

Also worth noting is that, while modalities like text messaging may be acceptable for patient use in some cases, provider-to-provider communication should only take place through entirely secure channels, such as team conversations on Spruce.

Bottom Line: The technology underlying secure messaging on Spruce is HIPAA-compliant.

SMS Text Messaging

You can also send traditional SMS text messages on Spruce. On your end, you still compose messages in the Spruce app, but your patients will receive them as standard SMS text messages from your practice's phone number. With this type of messaging, the patient does not need to download the Spruce app.

Like standard telephone calls, SMS is not something that Spruce or any other service can control completely, and there are fundamental aspects of the technology that would be unlikely to pass muster as technical safeguards under HIPAA. However, there are still easy ways to remain compliant with HIPAA while texting your patients.

If the following three criteria are met, the governmental guidance suggests that you should be in the clear to use standard text messaging with your patients in a HIPAA-compliant way:

1. The patient understands that standard text messaging (SMS) has security vulnerabilities

2. The patient understands that you provide secure alternatives to standard text messaging (such as Spruce secure messaging)

3. The patient still prefers standard text messaging over other options

Again, there is no explicit requirement to confirm in writing that these criteria have been met, but doing so would likely provide you extra protection. In the "Getting Patient Consent" section of this document, we have an example template that you can send to your patients.

For further detail, check out our blog post on texting with patients, HIPAA Compliance: Can I Text My Patients? Or read our dedicated white paper on using email and text messaging under HIPAA.

Bottom Line: Standard text messaging (SMS) on Spruce can be HIPAA-compliant but should be used with care and patient preference.

Telemedicine (Video Calls and Spruce Visits)

Telemedicine encounters on the Spruce platform are secure and can be used in a HIPAA-compliant manner.

Video Calls

All video calls on Spruce are encrypted to protect your PHI and other data. No recordings are made of the calls, and call information, such as patient identity and call duration, are logged securely for record-keeping and audit purposes for your organization. Because of this, they are straightforward to use in a HIPAA-compliant manner.

Spruce Visits

We also offer Spruce Visits, which are adaptive clinical questionnaires that you can send to patients who have the app downloaded. Spruce Visits are handled only within secure messaging conversations on the Spruce platform. Because of this, all PHI and other data contained in a Spruce Visit are subject to the same strict technical safeguards that we use for all secure messaging. We treat the content of every Spruce Visit as part of the patient's medical record, as we do with all communication on Spruce, and we protect it as such, in accordance with HIPAA regulations.

Bottom Line:	The technology underlying telemedicine on Spruce is HIPAA-compliant.

Phone Calls and Voicemail

Spruce lets you use your professional phone number on your personal cell phone, so that you can use one phone but keep all professional and personal communication separate — neither you nor your office staff or other colleagues have to give out any personal phone numbers. We also provide advanced telephony features, such as the ability to ring multiple provider phones when a patient calls and an automated after-hours answering service.

In order to get a patient's phone to ring, however, Spruce has to use the standard phone system for certain parts of our telephony feature set. This means that we don't control the information during every step of its journey, and neither does any other service that provides access to the phone system. The federal Department of Health and Human Services (HHS), which administers the HIPAA regulations, recognizes this and has codified the acceptability of typical voice calls under HIPAA in response to it. Your practice has likely not signed a BAA with the phone company for use of your office phones, and you won't need one for telephone service with Spruce either.

The exception for transmitting PHI as part of a standard voice call is narrow, though, and stored voicemails almost certainly will not qualify. That's why Spruce stores your incoming voicemails identically to other medical data, and you can be assured that they are protected by the same safeguards that we have in place for the rest of the system. We have also ensured the HIPAA compliance of our voicemail transcription process, should you choose to use this feature. Call logs and contact information, including patient names and phone numbers, are also stored securely in a HIPAA-compliant way on Spruce, without any leakage outside of the app. Taken together, these measures are likely to be significant protective advantages compared to any non-medical phone system you might have used.

Bottom Line: The technology underlying Spruce telephony, including voicemail storage and transcription, is HIPAA-compliant.

Email

Spruce allows you to send and receive unencrypted emails with your patients, as this is a communication channel that many patients prefer to use. There is a common misconception that medical practices must use encrypted email for all patient communication, but the government (HHS) has explicitly clarified that this is not the case:

> "The Privacy Rule allows covered health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so. [...] Further, while the Privacy Rule does not prohibit the use of unencrypted e-mail for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted e-mail."

Just as with standard SMS messaging, if your patient is aware that standard email has security vulnerabilities and also that you offer a secure communication alternative (such as Spruce secure messaging), then the direct guidance from HHS suggests that you may email that patient about medical issues without endangering your HIPAA compliance, so long as the patient prefers standard email over other options. Though it is not mandatory to confirm this in writing, it is probably a good idea, and we provide a template (Page 12) in this document that you can use with patients in the office to document their written consent and preference.

If you would like additional information on using email with patients, Spruce has also written a dedicated white paper on using email and text messaging under HIPAA.

Bottom Line: As with SMS messaging, standard email on Spruce can be HIPAA-compliant but should be used with care and patient consent.

eFax

Spruce supports eFax technology natively, and it is easy to use this powerful functionality to meet all of your faxing needs while remaining compliant with HIPAA. Importantly, Spruce stores your fax contacts and transmission logs, as well as digital copies of all of your incoming and outgoing faxes, identically to how we store all other medical data. This means that your fax information is protected by the same technical, administrative, and physical safeguards that HIPAA demands and that we use regularly throughout our entire system.

It is also important to note that, similar to phone calls, Spruce has to use the standard phone system for fax transmissions. This means that we don't control the information during every step of its journey, and neither does any other fax or eFax service. No need to fear, however: The federal Department of Health and Human Services (HHS), which administers the HIPAA regulations, recognizes this and has codified the acceptability of typical faxes under HIPAA in response to it, so it is straightforward to use Spruce eFax for HIPAA-compliant communication.

Bottom Line: The technology underlying eFax on Spruce is HIPAA-compliant.

Establishing Patient Preference

You can use the template below to document your patients' written consent and preference for the use of standard, unencrypted email and text messaging (SMS) for medical communication.

I, [Patient Name], hereby consent and state my preference to have my physician, [Physician Name], and other staff at [Practice Name] communicate with me by email or standard SMS messaging regarding various aspects of my medical care, which may include, but shall not be limited to, test results, prescriptions, appointments, and billing.

I understand that email and standard SMS messaging are not confidential methods of communication and may be insecure. I further understand that, because of this, there is a risk that email and standard SMS messaging regarding my medical care might be intercepted and read by a third party.

Inviting Your Patients to Spruce

Some Spruce features, including telemedicine and secure messaging, can only be used with patients who have created secure accounts on Spruce. There are two basic ways to invite patients to create such accounts—Spruce Links and standard invitations—and this section will explore both options through the lens of compliance so that you can pick which of them will best fit your needs. Either method can be used successfully and in a HIPAA-compliant way, however, so the choice between them represents workflow flexibility, rather than any type of quality hierarchy.

Spruce Links

Spruce provides you with a "Spruce Link," which is an organization-specific URL that you can give to your patients to let them create an account and connect automatically with your organization on Spruce. Spruce Links were designed specifically to be used in HIPAA-compliant workflows, and there are only a few key compliance considerations necessary for their proper implementation.

Most importantly, Spruce Links are secure. That is, once your patient has followed your Spruce Link, you do not need to worry about the account creation and connection process; this will all proceed securely and confidentially. However, you do need to carefully consider how you distribute your Spruce Link to patients when inviting them to connect with you, as an invitation alone can be enough to qualify as PHI.

Some common Spruce Link distribution methods are anonymous by nature, and these will typically be HIPAA-compliant without requiring any extra safeguards. Such anonymous distribution methods include, for example, putting your link on your website or making it available on printed handouts in your clinic. You can also get a QR code of your Spruce Link, so that people can scan it easily with mobile devices. You can set up your Spruce Link including getting your QR code under your settings, Secure Messaging and click on your Spruce Link. Read more about Spruce Links here. These methods don't involve patient identity, so it is simple to use them safely without improperly disclosing PHI.

On the other hand, if you would like to send your Spruce Link to a specific patient, you should carefully consider whether your accompanying invitation message constitutes PHI. A general-practice clinic might be able to send such a personal invitation without divulging health information, but if the name of your organization alone conveys something about a recipient's medical history, for instance, you should choose your method of transmission thoughtfully. Sensitive invitations should be sent securely, or by an insecure method only if the patient specifically prefers it.

You should also keep in mind that Spruce Links do not change, that each link can be used any number of times by any number of patients, and that anybody who has your Spruce Link can use it to make a secure patient account and connect with your organization on Spruce. These properties are essential to the usefulness of Spruce Links, but they also mean that you will need to carefully verify the identity and other information of every new patient who connects with you via a Spruce Link.

While Spruce verifies each user's phone number during account creation, all other demographic and contact information supplied by someone connecting through a Spruce Link will be accepted as entered, without verification. Because of this, we strongly recommend that you, at a minimum, make sure that each new patient's name and other account information matches your records and corresponds to their Spruce-verified phone number. You should also consider employing more stringent checks, as needed, such as confirmation calls or verification of secret information.

Learn more about how to use Spruce Links in our Help Center.

Standard Invitations

You can also use standard invitations to invite patients to create secure accounts and connect with your organization on Spruce. A standard invitation is essentially a one-time-use Spruce Link that you direct Spruce to send on your behalf, to a specific patient, via email or SMS text message. Please see our Help Center to learn more about using standard invitations. While standard invitations and Spruce Links share many of the same compliance considerations, there are several important distinctions that are important to note.

Most critically, standard invitations have a fixed format that cannot be altered and which includes the sending organization's name in the message text. As with invitations that include Spruce Links, you will need to decide whether it will be compliant for you to send such an invitation over an insecure channel like email or SMS text message. This decision is situation-specific and may depend on your organization's name, size, or medical specialty, or on other potential factors, such as those related to the patient you want to invite.

In general, your use of standard invitations on Spruce is more likely to be HIPAA-compliant if your organization's name and specialty do not inherently convey medical information, such as information about a specific health condition or field of practice. It will also be protective if your patient has expressed a preference for receiving medical communication via email or SMS text message.

In a further departure from Spruce Link functionality, when you instruct Spruce to send a standard invitation to a patient, the system will automatically send the invitation via email, SMS text message, or both channels, depending on what types of contact information you have provided for the patient in question. This can be a very effective behavior for reaching your patients, but you should ensure ahead of time that it will satisfy your compliance needs.

The inclusion of patient contact information in standard invitations raises compliance considerations, but it also offers an important security benefit that Spruce Links cannot. Specifically, the Spruce system will only allow a standard invitation to be used to create an account when a patient enters contact information that matches what you supplied for that specific invitation. This verification step provides you more control over who can connect with your organization, as well as more assurance that the identity of each connected patient is both correct and in agreement with your records.

As a final point of contrast with Spruce Links, after a patient has successfully used a standard invitation to connect with your organization, the invitation will become nonfunctional for any further attempted use. This may be a desirable behavior for certain workflows, as it allows you to more tightly control who can connect with your organization on Spruce, as well as when and how they can do so. In some situations, this may make subsequent identity verification easier and more reliable.

What Makes Spruce HIPAA-Compliant

If your organization is a covered entity, business associate, or subcontractor under HIPAA, then you know that you likely need to engage in a BAA with Spruce. As a reminder, there is a HIPAA-compliant BAA included automatically in the standard Spruce terms of service for organizations. This BAA gives you legal assurances that Spruce will protect your PHI, but you might be curious about the exact policies and procedures that we have in place to guarantee that we will do so.

In this section, we'll go through some of the nitty-gritty on the ways that we ensure that Spruce, as an organization, is secure and HIPAA-compliant, as well as the ways that we make sure that Spruce technology is straightforward for our customers to use in a manner that also keeps them compliant with HIPAA.

Third-Party Auditing and Certification

Spruce has completed a System and Organization Controls (SOC) 2 Type II audit examination. SOC 2 audits, performed by independent auditors, evaluate whether the safeguards and controls employed by organizations like Spruce are adequate to ensure the protection and security of their clients' data. For our audit, Spruce retained international business advisory firm Skoda Minotti, and we worked with their auditors to fully describe and document our systems and processes.

Skoda Minotti's testing of Spruce's controls included examinations of our policies and procedures regarding network connectivity, firewall configurations, systems development life cycle, computer operations, logical access, data transmission, backup and disaster recovery, and other critical operational areas.

Upon completion of the audit, Spruce received a Service Auditor's Report with an unqualified opinion, which signifies that the independent auditors found our policies, procedures, and infrastructure to meet or exceed the stringent SOC 2 criteria against which they were being assessed.

Spruce has also earned Certified status for information security by HITRUST for the Spruce core Care Messenger application, as well as its underlying infrastructure.

HITRUST CSF Certified status demonstrates that Care Messenger has met key regulations and industry-defined requirements and is appropriately managing risk. The HITRUST CSF assessment framework includes federal and state regulations, standards, and various third-party frameworks, such as HIPAA, NIST, ISO, and COBIT. For HITRUST certification, Spruce again worked with independent business advisory firm Skoda Minotti, with the final report being assessed and certified by the HITRUST Alliance.

Key Safeguards

Spruce maintains a standards-based risk management program to ensure that our services specifically support the requirements of HIPAA, including its provisions for administrative, technical, and physical safeguards.

Some key safeguards utilized by Spruce (list is not exhaustive):

- Spruce engages in a BAA with our storage and processing infrastructure vendor, Amazon Web Services (AWS), and only uses AWS services in ways that are compatible with this BAA. You can learn more about the controls and measures that AWS has in place to enable HIPAA-compliant services to be built on its infrastructure in this white paper.
- Spruce engages in a BAA with our major communications infrastructure provider, Twilio, and only uses Twilio services in ways that are compatible with this BAA. You can learn more about the controls and measures that Twilio has in place to enable HIPAA-compliant services to be built on its infrastructure on this site.
- Our servers are secured in a physical facility with round-the-clock surveillance, redundancy zones, multi-factor authentication, and security logging both at the application and infrastructure layer.
- We ensure unique user identification by requiring every provider to have their own account, enforced by two-factor authentication on every new device the provider uses.
- Our servers are hosted on dedicated instances that use hardware that has been isolated for our use.
- We employ best practices for network security, including having no system open to the Internet except for the load balancer that serves public facing requests for our website and API layer. All other components are contained in a virtual private cloud where we have access controls in place to ensure

- that we have minimum access open to each system necessary for the functioning of the platform. All network access is logged both for public-facing and intra-service communication. All access to our production systems are restricted to Spruce engineers and logged in an auditable format.

- All infrastructure used for storing and accessing data has measures in place to ensure not just data security but also data integrity.

- Our databases undergo automated periodic backups and can be automatically restored in the event of an emergency or failure.

- There is redundancy both at the application layer (with multiple instances of a service processing requests) and database layer (via replication across data centers) to ensure that we have a highly available platform and a contingency plan to quickly recover from failure.

- All data that we store in our systems is encrypted using leading industry-standard protocols (e.g., AES-256) at rest and in transit between our system and our users.

- Data stored locally on smartphone applications is limited to a minimum and kept only when absolutely necessary to enable core functionality of the software. Any and all PHI stored on smartphone applications is encrypted in transit and at rest on the device.

- All members of the team undergo ongoing HIPAA training.

- Spruce engages in BAAs with covered entities and subcontractors, as applicable.

Disclaimer

This document is not intended to and does not constitute the provision of legal advice with respect to the matters discussed herein. This document does not consider any state-based laws or regulations related to the privacy and/or security of personal health or other individually identifiable information. We encourage you to seek independent legal counsel to evaluate whether the use of SMS and/or email in your particular circumstances will satisfy your obligations under HIPAA as well as any state-based privacy and/or security laws or regulations.