



HIPAA-Compliant Texting:

How to Protect
Patient Privacy &
Your Organization





What to Know Before Reading This Guide

The Health Insurance Portability and Accountability Act (HIPAA) is a federal regulation that covers many aspects of patient health confidentiality. This guide is meant to serve

as one source of information to help you understand certain aspects of HIPAA—particularly how it pertains to text message communications within healthcare organizations.

This guide does not constitute legal advice. Please consult with your own legal counsel for standards and practices that are best suited for your organization.

Texting Has Become Mainstream in the Healthcare Industry

Did you know **83% of patients** say they would welcome reminders from their doctors about things like scheduling follow-up appointments, checking blood pressure, and taking prescribed medications? Additionally, **Black Book Market Research survey** of 770 hospital professionals and 1,279 physician practices found that secure texting has become a top choice for sending information while keeping sensitive data secured.

It's clear to see that texting has officially gone mainstream within the healthcare industry. In fact, health IT experts have even called text messaging **"the digital health tool of the century."**

So, it's no surprise that more and more healthcare providers today are incorporating text messaging into their daily communication practices. Whether it's used to keep medical staff informed with important updates while they're on the clock or to send patients helpful reminders, **text messaging serves as a fast and convenient form of communication that can make life easier for all parties involved.**

However, any healthcare provider who chooses to use SMS messaging as a communication method within their organization **must ensure their text messaging practices are in full compliance with HIPAA.** Without the deployment of appropriate security measures, the healthcare provider could place protected health information (PHI) at risk of exposure, hurt-

ing both patients and the provider organization (which could become subject to hefty government fines upon the occurrence of security breaches).

This is not to say that healthcare organizations should shy away from using SMS messaging within their organization, as it can be a valuable tool for **improving the efficiency of in-facility communication and enhancing operational workflow.** Furthermore, sending messages to patients on the communication platform they prefer can help them better manage their care. Therefore, **the optimal solution is for healthcare providers to employ systems and protocols that allow them to send text messages in a way that complies with the patient privacy standards established under HIPAA.**

RingRx is a HIPAA-compliant communication system that provides this type of infrastructure for healthcare offices, clinics, and organizations. However, even with HIPAA-compliant technology, healthcare providers must still take steps to use that technology the correct way so they do not violate the law.

To assist you in protecting both your patients and your organization, this guide provides information that demonstrates which types of activities do and do not constitute proper use of a HIPAA-compliant communication platform like RingRx. Below are examples of three different types of text communications to consider.

Secured vs. Unsecured Text Messaging

TEXTING ON RINGRX-SUPPORTED DEVICES (SECURED)

RingRx takes every precaution, where required by law, to protect data on or within its platform. Because all data stored on the platform is encrypted and use of the RingRx app requires credentialed login, any messages that arrive on a RingRx-supported device are protected. As a result, text communication between two RingRx subscribers (such as a doctor and nurse who are using the same platform) is fully secure, allowing for adequate protection of PHI and compliance with HIPAA. In this type of scenario, it is acceptable for two RingRx subscribers to discuss patient care via text message.

TEXTING TO MEDICAL STAFF'S PERSONAL CELL PHONES (UNSECURED)

Sending information to devices outside of RingRx (i.e., sending a text message to a medical staff member's personal cell phone) is not a protected service. This is because patient data on the receiving device is no longer within the service platform, and the data is therefore beyond RingRx's ability to control or protect. Sending information to devices outside of RingRx should be done only with a sound understanding of limitations under the law.

TEXTING WITH PATIENTS (UNSECURED)

Texting with patients is not secure because the patient's cell phone is outside of RingRx's platform. Therefore it is not possible to encrypt or secure the information on their cell phone or on the network services between RingRx and the patient, including the patient's cell phone service provider. Therefore, healthcare providers should be careful that text messages sent to patients do not include information that would be considered PHI. However, RingRx can safely be used to send non-medical information to patients, such as information about appointments, directions to the healthcare provider's facility, and other routine business matters.

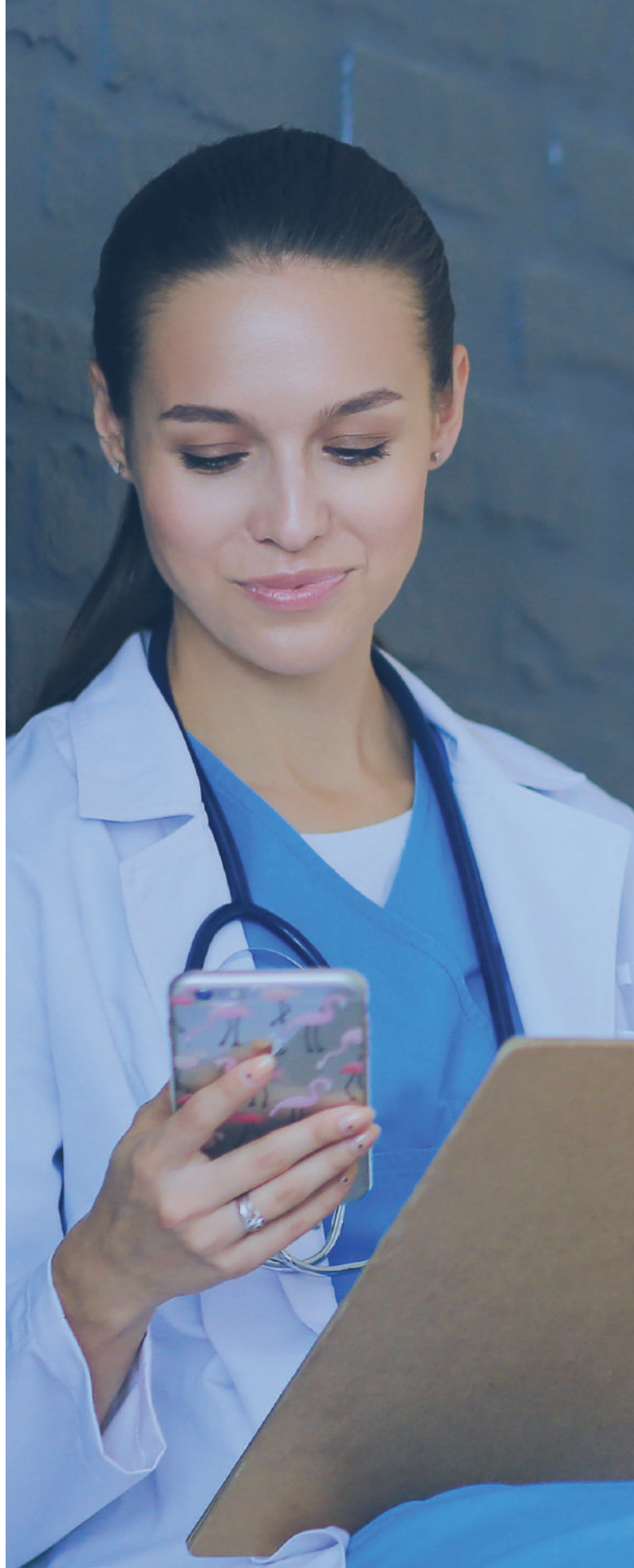
*In recent years, the Joint Commission and the Centers for Medicare and Medicaid Services (CMS) issued a **clarifying statement on texting**: "All health care organizations should have policies prohibiting the use of unsecured text messaging—that is, short message service (SMS) text messaging from a personal mobile device—for communicating protected health information." This makes it clear that PHI should not be communicated to or from a personal mobile device. Learn more about the position [here](#).*


Next Steps for Healthcare Providers

It is possible for healthcare providers to use SMS messaging to increase speed, efficiency, and convenience for themselves and their patients alike—it just requires the right technology combined with sound judgment in how that technology is utilized.

If you plan on using text messaging as part of your organization's communication practices, here are a few next steps to consider:

- Review your compliance policies to ensure your staff has proper guidelines as to what types of texting practices are and are not HIPAA-compliant.
- Obtain consent from patients who want to communicate by text, and make sure their consent is clearly documented.
- When you communicate with patients by text, only discuss topics that do not contain PHI (e.g., appointment reminders, directions, special promotions, etc.).
- If you choose to send messages containing PHI to patients (though this is not advised by RingRx), be sure to **warn them of the potential risks involved** and obtain their authorization for receiving these types of messages.
- If you have any uncertainties, consult your attorney before texting patients.





Boost Operational Efficiency While Keeping Patients Engaged

If you would like to create more efficient workflows for your organization and improve the patient experience, invest in a HIPAA-compliant communication platform that offers a wide variety of modern features. You wouldn't be alone—market research shows that 85% of hospitals and 83% of physician practices are using secure communication platforms to stay better connected with their care teams, patients, and patients' families. Additionally, be sure to

employ the best practices for protecting patient privacy discussed in this guide.

RingRx is an all-in-one platform that makes it easy for healthcare providers to comply with HIPAA for all their communication needs, including phone calls, text messages, faxes, and messaging sent through a desktop and mobile application. We offer customized solutions for healthcare organizations of all sizes. [Sign up for a free trial today!](#)