Clearwater

Whitepaper

From Texts to Telehealth

Common Risks & How to Reduce Exposures while using Tech Tools for Patient Communications

Table of Contents

Introduction

Communication expectations: understanding what patients and providers want and need

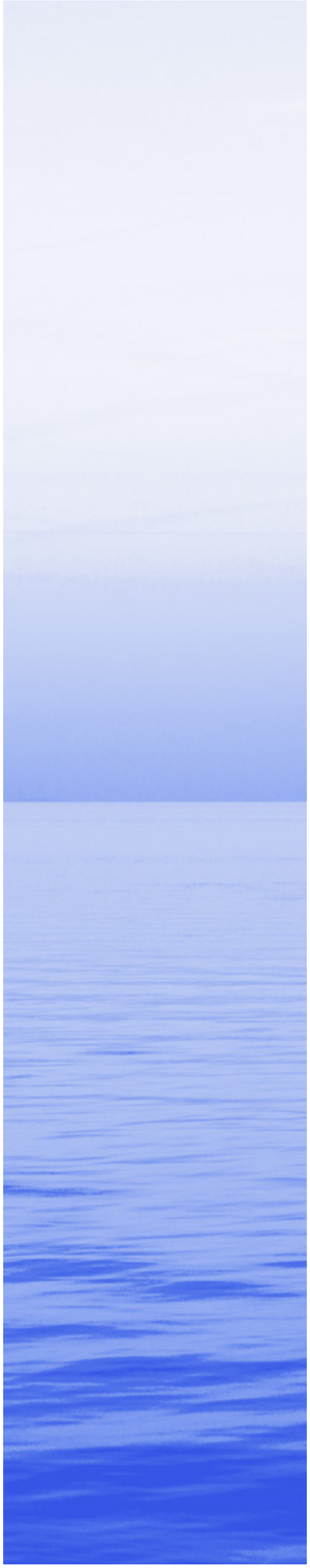
Technology has changed the way the world communicates and healthcare entities reap both benefit and burden related to available communications channels, speed of communication, and blurred lines between patient and provider expectations.

As people get more accustomed to instant communications in their personal lives via text messaging and social media connections, many expect the same opportunities when it comes to communicating with their healthcare providers.

And not only do they want more ways to communicate—phone call, text message, email, online forms, chats, and more—many have developed unrealistic expectations regarding provider response and capabilities.

While there are many efficiencies directly tied to expanded communication channels across so many platforms, what many patients may not realize is many of these tools are inherently unsafe for transmission of personal health information (PHI) or personally identifiable information (PII), and even fewer have likely ever thought about just what could happen if PII or PHI transmissions are breached or exfiltrated across unsecure channels.

As patients want to be more involved in their healthcare, including the ability to make more informed decisions, it's imperative they understand these risks and are well-versed in understanding provider obligation in relation to data security and HIPAA-compliant communications.



Ensuring compliant communication

Regardless of direction of communication, when patients and healthcare entities engage in an exchange of PHI, there are mandates that can help guide what should and should not be shared, which communication channels are secure, and what's expected regarding privacy and security.

For example, the HIPAA Privacy Rule covers all PHI, including ePHI. The rule can help direct compliant communications between providers and their patients, as well establish best practices to dictate record management and how much and what data is shareable.

You may be familiar with these guidelines in the form of a patient agreement where many entities detail their communication policies and procedures and request patients sign and acknowledge they understand both provider expectations as well as timelines and processes.

Similarly the HIPAA Security Rule can help a provider implement best practices regarding the confidentiality, integrity, and availability for keeping data secure and private.

The HIPAA Security Rule includes safeguards and controls to help ensure compliance, which is subject to audit, and should be routinely evaluated and tested by entitles to verify controls function as expected and meet HIPAA requirements.

The evolution of communications and the impact on healthcare

Texting and SMS

Today, if you spend more than a few moments with someone, you're likely to see the person engaging with a smartphone, sending and receiving text messages, scrolling social media, or responding to direct messages across a variety of public platforms.

With such rapid adoption and usage of cell phones for texting, it's hard to think not that long ago, our phones were still attached to cords and the only way to communicate was to place a call and chat with the person on the other end of the line.

In the early 1990s, as cellular phone adoption began to become more mainstream, Nokia introduced a service that would allow its phone to send and receive SMS, also known as simple message service. At first, SMS wasn't widely used, with, on average, most people sending less than one message a month in the United States.

But, nearly a decade later, more phones offered this service, and eventually expanded opportunities to send messages across competitor carrier networks. By mid-2005, as people became more used to the concept, the average number of texts per person rose to about 35 each month.

The biggest game changer appeared in 2007 when Apple introduced its first iPhone, rapidly expanding phone capabilities and adoption. Today, about 98% of Americans own some type of mobile phone, and there are more than 23 billion text messages sent each day around the world.

What we're seeing as a result is increased pressures from patients for providers to include SMS options for communication – for example, to schedule appointments and for appointment reminders.

When it comes to text messaging, most people think about SMS, which has a 160-character limit, but today, patients could also use multimedia messaging service (MMS), which allows exchange of data through pictures and videos; ; as well as over-the-top services (OTS), for example iMessage for iPhones; and a growing a number of secure messaging apps, such as WhatsApp or we chat, known as over-the-top messaging" to ". They may also use over-the-top services (OTS), for example iMessage for iPhones, and a growing a number of secure messaging apps, such as WhatsApp or WeChat, known as over-the-top messaging.

With the variety of texting options, many of which are not required to meet stringent privacy and security requirements as outlined by HIPAA, it's easy to see why there are a range of security and privacy risks with this preferred communication method.

For example:

- Message is not transmitted encrypted
- Can be compromised by providers/operators/governments
- Can remain on phone indefinitely
- Accounts are tied to the cell phone number
- No authentication required
- Can't guarantee who has the phone or if protected

Texting best practices

So what can you do to protect your healthcare entity from these texting risks when communicating with patients? Here are a few tips:

- Do
  - Have policies and procedures that establish parameters for patient communications via text
  - Determine if an application (particularly in an EHR) allows texting through a more secure mechanism and if you can capture data back into your into your records
  - Use company-controlled devices if you can, but if you allow BYOD (bring your own device) be sure you have enabled controls that allow your team to manage

    that device such as insight into data transmissions. It's also helpful if you enable capabilities that let you wipe the device if the employee leaves your organization

- Don't
    - Let employees use a personal device unless you have to
    - Give out a personal cell number to patients
    - Assume patient is consenting to messages in-kind. For example, if your patient communicates via text, you can't automatically assume it's OK to respond with PHI in the same manner. You must clarify and get consent.
    - Keep messages on devices once moved to official systems

Email

Before text messaging was a preferred communication method, email was king. While email picked up steam in the 1990s with the evolution of Hotmail, Yahoo mail, and AOL, email truly became mainstream when Google launched its email platform to the public.

And, as cell phone capabilities matured, so did the market for instantaneous email exchanges, where phones like BlackBerry even added physical keyboards to their devices to facilitate rapid typing for longer replies.

Like with text messaging, the evolution of the iPhone and mobile tablet devices took the ease and on-the-go benefits of email to the next level.

In 2020, for example, people sent and received more than 306 billion emails, which is expected to continue to grow in coming years, exceeding 376 billion by 2025.

Email risks

While email provides a number of benefits for healthcare entities, it's important to remember that most public email platforms are likely not secure enough to meet HIPAA standards. That's because, with email, for example, Simple Mail Transfer Protocol (SMTP), doesn't have built-in security. Unencrypted email is vulnerable at every stage—from sender to receiver.

Unfortunately, insecure email is also a prime target for would-be attackers who use things like phishing scams to gain credentials, launch malware, or initiate other breach methods.

Email best practices

If you use email to communicate with your patients, here are a few best practices you can employ to help decrease some of your risks:

- Do
  - Analyze and document email and video conferencing related risks and information about your entity's decision to use it for patient communications, keeping in mind the scope of your organization's risk analysis for HIPAA compliance, as well as your organization's risk threshold.
  - Use encryption. While you can't control your paitents' approaches to security and privacy, you can make suggestions to help protect their PHI. However, your time is likely better spent developing your own encryption policies, for example, encrypting data at rest, encrypting devices that could be stolen or lost, and establishing related procedures with your business associates.
  - Address back up and message retrieval
  - Determine how to audit
  - Ensure move to Designated Record Set (DRS)
  - Consider full encryption for devices
  - Determine need for business associate agreements
  - Develop and document related policies and procedures
- Don't
  - Share accounts: 1 person, 1 account
  - Keep messages on the platform once recorded in official systems
  - Use personal accounts for patient communications

Social media

One of the most common modern communication tools today is the use of social media. In the past several decades, we've evolved from bulletin boards and chat rooms to a gamut of social media tools that meet a range of interests and lifestyles from Instagram and Twitter to SnapChat, Facebook, Clubhouse, LinkedIn, and more.

One report indicates today there are more than 4.2 billion social media users globally, a figure that's increased by almost 500 million in the past year alone.

While social media is a great way to stay connected with people with a variety of interests and connections, many social media platforms don't have effective privacy controls and few have security and privacy practices that meet HIPAA standards.

But that doesn't prevent patients from using these resources to facilitate communications with healthcare providers, often with little to no awareness of just how unsafe that type of communication can be for PHI.

Social media best practices

If your healthcare entity has a presence on any web-based or social media platform, here are a few recommendations to help you reduce some of the risk communicating with patients this way:

- Do
  - Keep information limited to details the public needs to know about your practice, for example, public details such as office location, hours, and contact
  - If a patient reaches out to you via social media, keep the relationship professional. Remember the patient may choose to disclose PHI on the platform, but you're obligated to meet HIPAA standards.
  - Most social media platforms are all about data acquisition, so when using a social media tool to communicate with patients, be sure you know what kind of tracking mechanisms are in use
- Don't
  - Respond to social media posts (or things like Google or Yelp reviews) with any potential patient information
  - Accept friend requests or other personal social media connections with your patients without careful consideration
  - If a patient self-discloses PHI at will, don't respond in kind

APIs for data sharing

Most of our common social media apps use a range of application programming interfaces (APIs) that create communication pathways for applications to communicate with one another and share data. For example, if you play a game or take a quiz on a platform like Facebook, it's likely the game or quiz makers are using an API to facilitate that data exchange between their app and Facebook.

One report indicates that the number of AI Postman Collections (folders where API developer group API requests) increased more than 100% from 2019 to 2020, moving from 17.4 million to nearly 35 million. By January 2021, the number had already risen to more than 46 million collections.

Beyond common social media uses, the healthcare industry relies on APIs to help facilitate data exchanges through a huge array of applications and software that handle PHI and PII.

Here are a few examples of API usage in healthcare systems:

Patient access: Claims and other information shared through third-party apps (think insurance and payment tools)

Provider directory: For access to certain Medicaid and CHIP programs

Conditions of participation: For example, hospital electronic notifications

API best practices

Here are a few tips to help you decrease some of the risk of using APIs to communicate with your patients or transmit PHI or PII:

- Do
  - Understand compliance dates and requirements
  - Establish policies and procedures
  - Risk analyze and security test APIs
  - Monitor third-party app related threats
  - Establish business associate agreements with third-party vendors
- Don't
  - Ignore requirements or assume your vendor will handle them
  - Forget to document decisions regarding establishing and using APIs
  - Delay educating staff

Telehealth and video conferencing

Video conferencing is also experiencing an uptick in usage across many industries like healthcare, especially following the Coronavirus outbreak, which altered the way people engage with one another in public settings, even for much-needed appointments such as doctor visits.

While programs like Zoom, GoToMeeting, and FaceTime are common in modern work environments, you may be surprised to know that video conferencing has been around for much longer—as far back as 1936 when the first video telephone network was created. Today, a single video conferencing platform like Microsoft Teams, serves more than 75 million active users each day.

In healthcare, we've seen increased usage of these video conferencing tools, especially with the rise of telehealth and telemedicine as a result of the pandemic. Generally, like other digital communications methods, there is an expectation through HIPAA that providers will ensure these digital data exchanges are secure and HIPAA compliant. However, the Office for Civil Rights (OCR) eased some of its enforcement practices during the rapid adoption and implementation of telehealth services during the pandemic, giving some entities a bit of comfort in using insecure or public video conferencing tools.

For example during the pandemic, some providers chose to use non-public facing remote communication products such as Apple Facetime, Facebook Messenger Video Chat, Zoom, and Skype. It's important to note, however, that post-pandemic, OCR is expected to suspend this approach and all entities that want to continue to offer telehealth services will be expected to move toward secure and compliant tools.

Telehealth best practices

Instead of relying on non-compliant tools moving forward, here are some best practices to help decrease your telehealth and video conferencing risks:

- Do
    - Enable available encryption and privacy modes
    - Stop using all non-compliant platforms
        - Consider steps needed to move to compliant tools, including policies and procedures changes
    - Consider using HIPAA Compliant Products:
        - Microsoft Teams
        - Zoom for Healthcare
        - Go to Meeting
    - Get business associate agreements, if possible
    - Inform patient of privacy risks

        - For example, the risk that unencrypted messages can be intercepted
        - If the patient still wants text/email/video in an unsecure medium, proceed, but document their preferences and that they were warned about risks
    - Train and educate your staff on compliant practices and all policies and expectations
- Don't
    - Use public-facing communication products
        - Facebook Live
        - Twitch
        - Tik-Tok

Right of access initiative

Patient right of access is a high-priority today for OCR. While the initiative's goal is to ensure healthcare entities comply with patients requests for access to their medical records, the proliferation of new and common technologies certainly complicates communication practices between providers and their patients, often mudding expectations and capabilities.

For example, currently, if a patient requests records access, healthcare entities have 30 days to provide those records. However, a proposed change to the Privacy Rule could reduce that 30-day window to 15-days and could also widen the methods and ways patients make those requests, both orally and in writing, as well as outline expectations regarding response time and activity documentation.

Even without the proposed changes, we're already seeing an uptick in OCR patient right to access enforcement. At the end of March 2021, OCR announced it settled its 18th HIPAA Right of Access investigation, this one resulting in $30,000 in fines stemming from a patient complaint that the related healthcare entity failed to take timely action on a patient's record request.

These OCR enforcement penalties can have a significant negative impact on a healthcare entity or business associate, with to date penalties ranging from $3,500 to $200,000, with the average being about $65,000.

Some healthcare industry professionals say there is some ambiguity in the initiative and the industry needs more consistent guidelines – for example, regarding the definition of what a designated record set (DRS) is and what elements should be included.

Right of access best practices

While industry leaders work together to try to cut through some of the confusion, here are some tips that may help you avoid some risks related to patient right of access:

- Do
  - Formally define (in policy) data elements and record systems
  - Ensure all data in your DRS is in-scope
  - Consider any record used to make a decision about patient
  - Identify location of paper records and medical device output
- Don’t
  - Forget about emails and texts that must also be captured
  - Forget billing and other types of records
  - Delay responding. Remember, you must respond within 30 days, with one 30-day extension possible, but this could soon change to a 15-day response window possible

Reducing communication risks

As technology continues to evolve and patient expectations change, providers will continue to face risks and challenges related to effective, prompt, and secure patient communications.

Regardless of which tool you use, here are a few important takeaways:

- If the data identifies (or may identify) the individual as a patient, then it is PHI, and compliance requirements apply
- Confidentiality, integrity, and availability are required, no matter the platform or communication channel
- Applications and services may be able to access messages and information transmitted across their platforms, rendering them insecure options for PHI exchanges
- Consider establishing business associate agreements with technology providers (unless the narrow “conduit exception” applies)

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact