Using SMS and Email under HIPAA

The use of digital communication is undeniably changing healthcare delivery. Increasingly, physicians are using text messaging (SMS) and email to send information to both colleagues and patients, and recent research has found that in some settings upward of 90 percent of doctors are using text messaging to manage patient care.

Despite widespread use, however, the legality of communicating via text and email with patients is still a point of confusion for physicians and other providers, especially in light of regulation imposed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In reality, there are many situations in which the use of text and/or email to communicate with patients will not violate HIPAA.

"...in some settings upward of 90 percent of doctors are using text messaging to manage patient care."

To help physicians navigate the tension between the need to protect patient privacy and the value of text and email in the modern healthcare system, let's take a careful, honest look at the facts.

Why are Text and Email so Important?

Text and email are important to providers because text and email are important to patients. The expectation of mobile access has become the norm in most aspects of consumer life, and healthcare is no exception. In a 2015 John Hopkins study, researchers found that 37 percent of patients had used their personal email to contact their doctors or hospital within the past six months, and 18 percent reported using Facebook for the same purpose. At the same time, patient portals designed to field this communication have failed to gain traction—data published by CMS indicate that 66 percent of hospitals had zero patients attempt to access patient portals in 2015. Despite being positioned as a direct alternative to text and email, portals in their current form lack the frictionless adoption, no-sign-in login, and mobile-first functionality that make text and email so attractive and intuitive to patients.

There is also strong evidence that the use of text and email in healthcare delivery has a positive impact on patient outcomes and quality of care. A systematic review published in 2015 by the Annual Review of Public Health found that almost all text message interventions were effective in improving health outcomes and behaviors among studied participants. Text messages were found to be particularly impactful when addressing chronic conditions, such as diabetes self-care, weight loss, smoking cessation, and antiretroviral medication adherence.

When is it Okay to Use Text and Email?

Physician concerns around the use of text and email for patient communication arise from uncertainty about where HIPAA stands on the issue. In fact, neither text nor email communication are specifically prohibited under HIPAA. The US Department of Health and Human Services (HHS) has described, in FAQs and commentary, situations in which providers may (and in some cases should) use such channels to communicate with patients.

"...almost all text message interventions were effective in improving health outcomes and behaviors..."

To better delineate when one should and should not use text and email, let's examine four common scenarios where these modalities are permissible:

Scenario 1: Patient initiates communication over email or text

> **If a patient initiates health-related communication with a text or email, the provider can assume that the patient finds communication via that channel to be acceptable and can respond via text or email.**

This conclusion is based on an FAQ published by HHS regarding electronic communications with patients.

Importantly, providers should still use reasonable safeguards when continuing text or email communication, such as always ensuring that it is actually the patient behind the email address or phone number that initiated the contact. Further, in utilizing such communication, providers must still comply with the requirements of the HIPAA Security Rule.

"...providers should still use reasonable safeguards when continuing text or email communication..."

Additionally, if a provider feels that a patient may not be aware of the risks of unencrypted text or email, they should send a short notice of those risks to the patient so that they can make a fully-informed decision.

Scenario 2: Patient gives formal consent before any text or email exchange takes place

When a patient has explicitly consented to communication with their care team over text or email, a provider is free to send texts or emails that contain PHI.

The use of unencrypted email in such a case was clarified by HHS in published commentary to the 2013 HIPAA Omnibus Rule. A provider can send a patient unencrypted email (and presumably texts) when the provider has done the following:

- Provided warning that unencrypted emails and texts may be insecure;
- Advised the patient of the risks of unencrypted emails and texts (the provider doesn't need to get into the details of encryption technology; he or she merely needs to explain that there is some risk of the messages being read by a third party); and
- Received confirmation from the patient that he or she "still prefers" to receive communication via text or email, notwithstanding the risks.

In this scenario, explicit patient consent should be documented to manage the provider's liability—it is not enough to notify the patient and then assume that their silence is equivalent to consent. Below is a template that can be used to document consent before using text or email 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.*

As in the previous scenario, providers should always implement reasonable safeguards before using any communication method. Furthermore, this type of consent only applies to communication between a provider and the patient; all provider-to-provider communication must still be secure and HIPAA-compliant.

Scenario 3: Patient requests that provider communicate via text or email

> **Under the HIPAA Privacy Rule, patients have the right to request that their provider communicate with them via their preferred means, and providers are obligated to accommodate these requests, if reasonable.**

As in Scenario 1, HHS has published an FAQ on this. They offer the example of a patient who requests to receive appointment reminders by email rather than postcard and state that the provider not only may but should accommodate the patient's request to receive reminders via email,

assuming that email is a reasonable alternative means of communication for their practice.

Note that the inverse of this guidance is also true: if a patient requests not to receive communication containing PHI by email or text, then a provider should offer and accommodate alternate channels of communication that are more secure, such as postal mail or telephone.

Scenario 4: Provider sends a text or email when the patient hasn't provided consent and did not initiate the communication

Providers may be able initiate communications by text or email even when the patient hasn't provided consent so long as the communication does not contain any PHI, and otherwise complies with HIPAA requirements regarding permissible uses of PHI.

If a patient has neither provided consent nor initiated communication by text or email, providers may still be able to these channels for communication so long as they ensure that their messages are not individually tailored to a particular patient, do not contain any PHI and otherwise comply with HIPAA requirements regarding permissible uses of PHI, including with respect to marketing. By nature, all messages contain some personal information, such as a unique phone number, email address, or recipient name. The content of any message must therefore be considered in conjunction with these details, and the totality must not constitute PHI (or otherwise violate HIPAA requirements regarding how a provider can use PHI).

"If a patient has neither provided consent nor initiated communication by text or email, providers may still be able to these channels for communication..."

By way of example, consider a

provider sending an email or text to a patient that says, "It's flu season—have you gotten your flu shot?" Even though this message is clearly linked to the patient, it may not qualify as PHI because it is broad, non-personal information that could apply to anyone. The phrasing of the message, however, is crucial. If it instead said something like, "This is a reminder that you're overdue for your flu shot," it would become PHI, since it reveals that the patient has not yet gotten the shot. The generic wording of the first message makes it applicable to anyone and thus renders it unlikely to be PHI. An important caveat is that practices in highly specialized or sensitive fields, such as cosmetic surgery, must be especially careful, as any communication that identifies an individual as a patient of the practice could be construed as revealing medical history and would therefore constitute PHI. In addition, HIPAA imposes certain requirements regarding how a provider may use PHI in its possession, including for purposes of general marketing, so it is critical to ensure that any such emails or texts are consistent with the provider's Notice of Privacy Practices and obligations under HIPAA.

If in doubt as to whether a text or email contains PHI, consider what would happen if a third party who knows the patient picked up the patient's phone and saw the text or email: would that third party then know something about the patient's medical history? If so, the messages contains PHI.

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.

Sources

1. Plant, M. A. & Fish, J. S. Resident use of the Internet, e-mail, and personal electronics in the care of surgical patients. *Teach. Learn. Med.* **27**, 215–223 (2015).

2. Lee, J. L. *et al*. Patient Use of Email, Facebook, and Physician Websites to Communicate with Physicians: A National Online Survey of Retail Pharmacy Users. *J. Gen. Intern*. Med. 31, 45–51 (2016).

3. Patient Portals Still Struggling To Engage Users. *HIStalk Connect* at <http://histalkmobile.com/patient-portals-still-struggling-to-engage-users/>

4. Centers for Medicare & Medicaid Services (CMS). *CMS Electronic Health Record (EHR) Incentive Program Eligible Hospitals Public Use File (PUF) Data Dictionary and Codebook.* (Centers for Medicare & Medicaid Services (CMS), 2013). at <https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EH_PUF_Codebook_June.pdf>

5. Hall, A. K., Cole-Lewis, H. & Bernhardt, J. M. Mobile text messaging for health: a systematic review of reviews. *Annu. Rev. Public Health* **36**, 393–415 (2015).

6. U.S. Department of Health & Human Services. 570-Does HIPAA permit health care providers to use e-mail to discuss with their patients. *HHS.gov* (2008). at <http://www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/>

7. Office for Civil Rights, Department of Health and Human Services. 45 CFR Parts 160 and 164: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules. *Fed. Regist*. **78**, 5566–5702 (2013).