DIGITAL ENGAGEMENT DEMANDS A NIMBLE HIPAA STRATEGY

By Jill DeGraff, JD; Helen Pfister, JD; and Randi Seigel, JD

Mobile apps, e-mail, and text messaging present new opportunities for health plans and health care providers to engage their members and patients. However, organizations must keep in mind that sending electronic protected health information (ePHI) through these channels poses HIPAA risks.

Because sensitivity of the information being conveyed and the choice of communication pathway varies by use case, HIPAA requires organizations to evaluate the benefits, risks, and mitigation strategies for specific operating environments. Consequently, organizations need a process to thoughtfully consider each case to optimize their digital engagement strategies.

HIPAA

HIPAA governs, among other things, the security of ePHI created, maintained, transmitted, and received by a covered entity (CE). CEs include health care providers, health plans, and health care clearinghouses. While encrypting ePHI protects CEs from sanctions under HIPAA should a breach occur, HIPAA does not categorically prohibit transmitting unencrypted ePHI. If a CE elects to permit unencrypted transmission (via e-mail or text message), the CE must implement safeguards that are "reasonable and appropriate" and document that an "equivalent alternative measure" has been implemented.

Unfortunately, Health and Human Services provides little guidance about the alternative measures deemed to be an equivalent safeguard when an e-mail, text message, or mobile app contains ePHI. The only guidance was issued in the preamble to the 2013 final HIPAA Security Rule, where Health and Human Services clarified that a CE does not violate HIPAA by e-mailing ePHI at an individual's request after advising the individual of the security risks. For this reason, obtaining consent to receive ePHI and advising of the security risks is fundamental to any "equivalent alternative measure."

Mobile Apps

Consent for exchanging ePHI on a mobile app can be obtained when a user downloads the app and accepts its terms of service. Secure mobile apps are well utilized due to a user's familiarity with mobile app workflows and capabilities. CEs also benefit from enhanced features that mobile app developers bring to market and their use of cloud-based platforms to deliver state-of-the-art security and computing power. Many developers allow CEs to conserve resources by starting with small pilots.

However, as the portfolio of mobile apps grows, so, too, do a CE's compliance responsibilities. CEs need to ascertain how well each mobile app vendor understands its HIPAA responsibilities and maintains a HIPAA-compliant environment. Some CEs may also be concerned that mobile apps carry hidden costs due to low adoption rates, particularly among nonsmartphone owners.

E-mail

E-mail offers different advantages. It's accessible to anyone with an e-mail account, and the contents can be uploaded to EHRs. Organizations have the option to encrypt. If they choose not to encrypt, a patient or a plan member can e-mail without having to use a specific program.

However, e-mail presents unique risks inherent to the internet. Servers that maintain e-mail copies present opportunities for their contents to be compromised. Also, issues with integrity control arise because a malicious actor can change or divert e-mail without detection. However, if encrypted e-mail is utilized, adoption may be lower because a recipient first needs to install a program.

Organizations can mitigate risks by defining a process for verifying individuals' identities, obtaining their consent, and advising them of the security risks. They can also limit the types of ePHI that can be communicated by removing patient names, initials, and medical record numbers from subject lines, ensuring sensitive information such as Social Security numbers is never included in any e-mail correspondence, and limiting the information that appears on a locked screen.

Text Messaging

Text messaging may offer advantages over e-mail and mobile apps because it generally has high open and response rates. Also, text messages can be transmitted over SMS networks to any person with a cellular phone (not just a smartphone).

In terms of security, cyberthreats are difficult to execute in an SMS text messaging environment. Text messages can be read only on the device to which a wireless number is assigned, and protective measures similar to those used for e-mail can be applied to text messaging.

The Federal Communications Commission regulates SMS text messaging under the Telephone Consumer Protection Act, which requires organizations to obtain recipients' prior express consent before sending them text messages. The act permits prior express consent to be implied when a person knowingly releases his or her phone number to the CE and the text message is reasonably related to the original purpose for which a number was provided. However, the guidance is unsettled regarding how closely related that purpose needs to be with the message.

Balancing Benefits and Risks

Although HIPAA complicates the use of apps, e-mail, and text messaging, the compliance burden is often outweighed by the benefits of inspiring consumer satisfaction and loyalty at little cost. In general, health plans and health care providers that successfully navigate these patient engagement strategies share the following three traits:

- a compliant culture;
- a well-defined governance framework; and
- a thoughtful approach to managing the business associate/technology vendor relationship.

Strong Culture of Compliance

A strong HIPAA-compliant culture integrates an organization's privacy values throughout its workforce, technology, and clinical and business processes. Once an organization is comfortable with its HIPAA compliance, it can move from categorical prohibitions of exchanging ePHI through these channels to a nuanced application of HIPAA that considers the benefits, risks, and mitigating strategies in individual use cases.

Well-Defined HIPAA Compliance Framework

Privacy professionals must be not only HIPAA experts and enforcers but also policy conveners who develop strong governance frameworks for digital engagement. Elements of these frameworks may include the following:

- **Advisory committees.** Seek the input of practitioners, business leaders, and members/patients. Include representation from clinical, staff, marketing, legal, compliance, information systems, and finance.
- **An understanding of consumer needs.** Make sure that use cases reflect an understanding of the reasons for exchanging ePHI and why members or patients welcome receiving it through a chosen medium.
- **Policies and procedures.** Develop a HIPAA policy that defines standards and a process for considering new technologies. Allow policies and procedures for specific uses to evolve based on feedback from earlier implementations.

Managing Business Associate Technology Vendors

Many organizations will not implement a formal e-mail, text messaging, or mobile app initiative without a technology vendor (even if it's only a cloud provider). The sophistication of technology vendors varies. Therefore, a thoughtful and thorough process is needed to evaluate the HIPAA compliance fitness of each vendor.

CEs must establish routine procedures for evaluating vendors, document their findings, and negotiate business associate agreements—not just the underlying service agreement—to reflect each vendor's uniqueness and the ePHI at risk. Among other things, contracts should confirm who owns the data, how the data may be used, how the CE will be indemnified for a HIPAA breach, and the timeframe for notifying the CE of breaches.

CEs also must actively monitor and audit their technology vendors for compliance.

Conclusion

To take advantage of mobile apps, e-mail, and text messaging, CEs must adopt an agile mindset. By developing governance standards and guidelines, CEs can become more confident in adopting new technologies, which should advance certain strategic objectives.

— Jill DeGraff, JD, is a partner at Manatt Health, a division of Manatt, Phelps & Phillips, LLP, a fully integrated, multidisciplinary legal, regulatory, advocacy, and strategic business advisory health care practice.

— Helen Pfister, JD, is a partner at Manatt Health.

— Randi Seigel, JD, is counsel at Manatt Health.