Published on *The National Law Review* https://natlawreview.com

Communications Compliance: Are Messaging Applications Leaving Your Organization Vulnerable to HIPAA Liability?

Article By:

Vinay Bhupathy

Messaging applications are popular tools to facilitate communication and workflow in healthcare settings—increasingly so as smart phones, tablets and other mobile mediums continue to penetrate the market. Organizations relying on or acquiescing in the use of informal messaging platforms, however, should be aware of the risk for data breaches and other ***HIPAA*** liability.

As between healthcare providers, messaging activity conducted over standard consumer communication platforms implicates a number of common HIPAA concerns including the loss or theft of devices with stored protected health information, the lack of encryption, use of the technology in public spaces and network security. It is worth noting that related penalties can add up quickly given that, under HIPAA, each instance of unsecured exchange constitutes a separate event subject to a penalty.

Despite the potential consequences, a recent survey conducted by a mobile messaging services developer highlights a lack of awareness and confrontation of the issue among executives and employees.[1] Only 8% of respondents indicated that their company prohibits the use of third-party messaging platforms, fewer than 50% indicated that their company has an official platform and, among those that do, a combined 27% adopted GChat or WhatsApp as the platform. 30% of respondents believed that corresponding through such platforms is completely secure while another 42% believed that it is generally secure.

Are healthcare facilities thereby relegated to pagers and other more traditional forms of communication? Certainly not. The standards of the HIPAA Security Rule are “technology neutral,” meaning that compliance turns on systems of safeguards as opposed to the implementation (or avoidance) of specific technologies. A HealthIT.gov FAQ, for example, notes that an organization “may approve texting after performing a risk analysis or implementing a third-party messaging solution that incorporates measures to establish a secure communication platform that will allow texting on approved mobile devices.”[2]

Compliance policies and practices are, therefore, essential. Organizations should adopt, disseminate, and train staff regarding an official position on the use of messaging applications. For organizations interested in authorizing messaging activity, a growing number of vendors offer platforms designed

with HIPAA and the secure transmission of protected health information in mind. Suitability likely depends on the needs, size and complexity of a given entity—considerations such as whether the organization limits the use of personal devices and whether more restricted or expansive messaging capabilities are required. The right system, adopted as part of a comprehensive risk management strategy, can help organizations achieve the ease and efficiency of messaging communication without undue HIPAA liability exposure.

As we anticipate enforcement efforts on the part of the Office of Civil Rights to continue with full force in 2016, organizations that have not yet addressed messaging activity and the transmission of protected health information are advised to do so now.

Rachel Landauer is co-author of this article.

---

[1] The study findings are available here.

[2] The FAQ is available in full here.

National Law Review, Volume V, Number 334