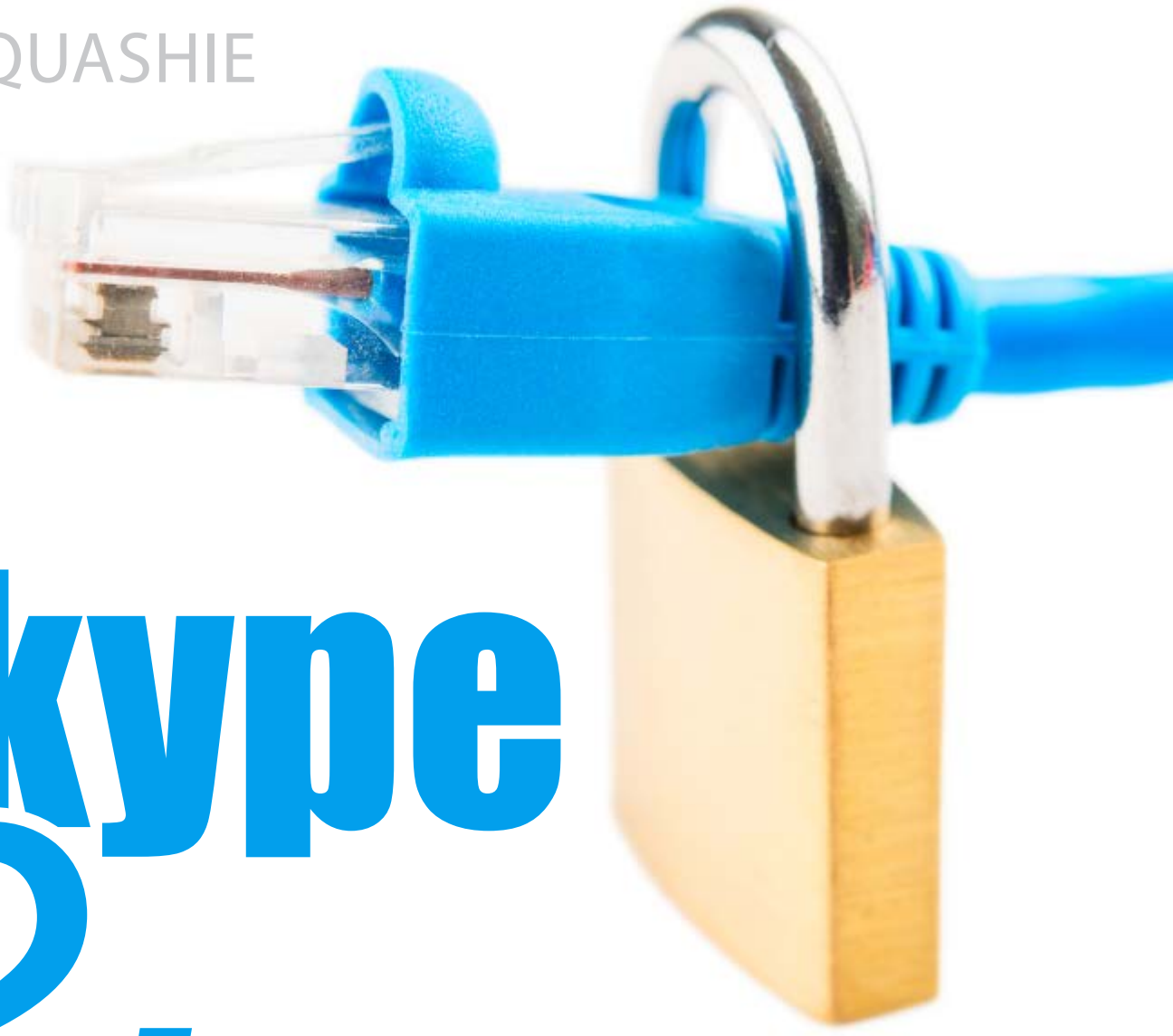
RENÉ QUASHIE



Skype & HIPAA

The Vexing Question

Skype

and similar web-based platforms are increasingly becoming a way for many physicians and other health care practitioners to communicate and interact with patients at a distance. Many telehealth practitioners in particular use web-based platforms for the delivery of care and communications with patients—especially in certain telehealth subspecialties such as telepsychiatry. The reasons are clear. Skype is essentially free—there is no charge for making calls to other Skype users, although there are fees for making calls to mobile and landline telephones. Skype is also ubiquitous. Skype alone is estimated to have approximately 600 million users worldwide, and its many users rely on Skype to communicate with professional associates, family, and friends. These figures do not even take into account users of other platforms that are proving popular with consumers and professionals alike. In other words, web-based platforms are easy to use and readily available.

Nevertheless, the issue of whether to use Skype or similar web-based platforms is a vexing one for many health care providers.[1] Notwithstanding the fact that Skype is ubiquitous, its use may be inappropriate for health care providers as communication and treatment via web-based platforms raise a number of significant HIPAA privacy and security issues:

Many platforms are proprietary, meaning that health care providers have no way to determine if and what information is stored.

Users cannot reliably develop and verify an audit trail.

There is no reliable way to verify transmission security.

Users have no way to know when a breach of information occurs.

There is a lack of integrity controls to ensure that electronic protected health information is not altered.

By way of quick background, the Health Insurance Portability and Accountability Act and its resulting regulations pertaining to privacy and security ("HIPAA") require covered entities, such as health care providers, to protect the confidentiality of protected health information, and guard against unauthorized access, use, and disclosure of such information.[2] Among other things, HIPAA rules require (or make addressable): [3]

Access controls
implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access.

Audit controls
implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Integrity
implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Person or entity authentication
implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Transmission security
implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Security management
implement policies and procedures to prevent, detect, contain, and correct security violations.

Assigned security responsibility
identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

Information access management
implement policies and procedures for authorizing access to electronic protected health information.

Security incident procedures
implement policies and procedures to address security incidents, including identifying and responding to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

Breach notification
Report notification of any breaches of unsecured protected health information to affected individuals, the Department of Health and Human Services (HHS), and, in certain circumstances, to the media.

The use of web-based platforms, especially those that are proprietary, makes it difficult for health care entities to meet many of their HIPAA obligations. In other words, telehealth providers may carry a higher risk of potentially violating HIPAA rules when they use web-based platforms such as Skype. In the current regulatory climate, not meeting HIPAA requirements carries greater significance than before given the significant increase in HIPAA enforcement activity.[4]

Recently, a number of organizations (including Open Technology Institute, Reporters

Without Borders) signed an open letter to Skype which, among other things, requested that Skype publicly release:

- Quantitative data regarding the release of Skype user information to third parties, including the number of requests made by governments, the type of data requested, and the proportion of requests with which it complied.
- Specific details of all user data Skype currently collects.
- Its data retention policies.
- Skype's view of what user data third-parties may be able to intercept or retain.
- Skype's policies related to the disclosure of call metadata in response to subpoenas, and its policies and guidelines for employees when Skype receives and responds to requests for user data from law enforcement and intelligence agencies in the United States and elsewhere.

The letter highlights the security concerns consistently voiced by many within the privacy and security community. Indeed, late last year, a security flaw was uncovered which allowed Skype accounts to essentially be hijacked—enabling would-be hackers to sign up to Skype with email addresses already being used by other Skype users and force password resets for any accounts associated with those emails.

For these reasons, many leading information security organizations generally recommend against the use

of Skype and similar platforms for communications involving health information. These organizations have concluded that web-based platforms are not secure, and are an inappropriate way by which to communicate with patients—given that health information is often times exchanged in such encounters.

None of the concerns highlighted, however, mean that a telehealth professional should not use Skype to engage with patients—only that they understand the greater liability risks involved. For telehealth providers who decide to use Skype, there are a number of considerations they should review to better protect themselves from potential HIPAA liability:

- Request audit, breach notification, and other information from web-based platform providers.
- Have patients sign a HIPAA authorization and a separate informed consent as part of intake procedures.
- Develop specific procedures and protocols regarding use of web-based platforms (interrupted transmissions, backups, etc.).
- Formally train the workforce on the use of these platforms.
- Exclude the use of these platforms for vulnerable populations (i.e., severely mentally ill, minors, those with protected conditions such as HIV).
- Limit to certain clinical uses (i.e., only intake or follow up).
- Use secure platforms with audit trail, breach notification, other capabilities.

Even if practitioners take these and other steps it may not insulate them from potential HIPAA liability (not to mention state privacy and security laws). Thus, to the extent that a provider can use fully encrypted, non web-based and secure technology, they should do so. These services are usually not free, however. But the fact that Skype is free does not make it appropriate for use by health care practitioners.

ABOUT THE AUTHOR

René Quashie is Senior Counsel in the Washington D.C. office of Epstein Becker and Green where he focuses on health care regulatory matters and health care policy. He is also a member of the Legal Resource Team at the Center for Telehealth and eHealth Law.

[1] For purposes of this article, the term "Skype" will be used to include Skype and similar free web-based communication platforms relying on proprietary voice over Internet technology. Note that Skype and similar platforms are proprietary services.

[2] 45 C.F.R. Parts 160 and 164.

[3] 45 C.F.R. §§ 164.308, 164.312, 164.404-410. "Addressable" means that the entity use reasonable and appropriate measures to meet the standard or it can decide the standard can be met without the implementation of an alternative—but it must document this conclusion.

[4] According to the HHS Office of Civil Rights, the agency entrusted with primary HIPAA enforcement, complaints regarding potential HIPAA violations reached all all-time high in 2011, the last year for which data is available. (http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/complaintsyear.html)