Nefsis Video Conferencing and HIPAA

Health care entities and providers use video conferencing to improve efficiency and reduce travel costs for both themselves and their patients. Consultations held as online meetings between providers, or between providers and patients, afford privacy, security and real-time interaction, without the inconvenience of traveling or waiting.

Wherever healthcare and technology overlap, questions about the Health Insurance Portability and Accountability Act (HIPAA) inevitably arise. Title II of HIPAA deals with the privacy and security of electronic healthcare transactions and sets out criteria for compliance.

> ***In short, Nefsis is not a health-related business or a "covered entity" under HIPAA, nor is it a "business associate" of a covered entity under the Health Information Technology for Economic and Clinical Health Act (HITECH Act). Covered entities and their business associates may securely and privately use Nefsis in healthcare-related video conferences. While control over the selection of content shared by users in an online meeting rests with those covered entities and business associates, Nefsis helps them comply with HIPAA.***

Overview of HIPPA

Title II of HIPAA includes five rules of "Administrative Simplification" for making health care more efficient and medical information more accessible, and two of them – the Privacy Rule and the Security Rule – relate to electronic data communication.

HIPAA and the Department of Health and Human Services (HHS) define the "covered entities" to which these rules apply: health plans; health care clearinghouses, such as billing services and community health information systems; and health care providers that transmit health care data in electronic form.

> ***Since Nefsis does not fall into any of these categories, it is not a covered entity under HIPAA.***

How HIPAA relates to video conferencing

The Privacy Rule governs the ways in which information about a patient's health status, treatment and payment is used and disclosed. The rule applies to covered entities – not to providers of video conferencing services – and requires them, among other things, to take reasonable steps to ensure confidentiality in communicating this information.

The Security Rule sets out standards for keeping Electronic Protected Health Information (EPHI) safe. Of note is its Technical Safeguards provision, setting rules for access to computers and the secure communication of EPHI over public networks to protect it from interception by anyone other than the intended recipient.

Again, compliance with these safeguards rests squarely with the covered entities who, under 45CFR164.312, must "implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network." As they relate to video conferencing, these measures include "a mechanism to authenticate EPHI," "a mechanism to encrypt and decrypt EPHI," and "policies and procedures to protect EPHI from improper alteration or destruction."

Authentication

Authentication is the process of verifying that an entity – user, administrator, conference participant, computer, conference server – is who or what it claims to be.

> ***Nefsis lets conference hosts select secure conferencing with conference room passwords. In all Nefsis video conferences, users must deliberately go out through their firewall to log in, and there is an option to dial out to participants, instead of their dialing in. Conference hosts recognize and can check every meeting participant, and can expel any participant at any point in the conference.***

Encryption

Encryption keeps the video conference private and prevents eavesdropping.

> ***Nefsis' secure conference settings require an SSL3-/TLS-encrypted connection for all users prior to joining, and they encrypt connections from end to end, including all participants and the conferencing server. Nefsis also sends all conference data – live data sharing, presentations, Voice over Internet Protocol (VoIP) and video – over one secured TCP/IP connection. Nefsis secures the video conference and helps covered entities comply with HIPAA, with no noticeable effect on video quality.***

Integrity

A third measure relates to securing access to and preserving the integrity of EPHI.

> ***Nefsis gives users the option of storing conference content – live data sharing, presentations, Voice over Internet Protocol (VoIP) and video – that could be regarded as EPHI. Covered entities choosing to save videoconferences for inclusion as EPHI may safely record Nefsis content to their own HIPAA-ready electronic health record (EHR) system. By choosing not to store conference content on Nefsis servers, covered entities will comply with guidelines relating to the integrity of medical information.***

Conclusion

Since a company providing video conferencing services, like Nefsis, is not a covered entity or a business associate of a covered entity under HIPAA, there are no particular rules to observe. Nevertheless, Nefsis helps these entities maintain HIPAA compliance by protecting patient privacy in their video conferences and online meetings.

With its high standards of authentication and encryption, Nefsis exceeds the Technical Safeguards of HIPAA's Security Rule. As for guidelines on the integrity of health information, covered entities may safely store Nefsis conference content in any HIPAA-ready EHR system.

# # #