National Telehealth Resource Centers (NTRCs):

National Telehealth Policy Resource Center
www.telehealthpolicy.us

National Telehealth Technology Assessment Resource Center
www.telehealthtechnology.org

Regional Telehealth Resource Centers (RTRCs):

California Telehealth Resource Center (CA)
www.caltrc.org

Great Plains Telehealth Resource and Assistance Center (ND, SD, MN, IA, WI, NE)
www.gptrac.org

Heartland Telehealth Resource Center (KS, MO, OK)
www.heartlandtrc.org

Mid-Atlantic Telehealth Resource Center (VA, WV, KY, MD, DE, NC, PA, DC)
www.matrc.org

NorthEast Telehealth Resource Center (CT, MA, ME, NH, NY, RI, VT)
www.netrc.org

Northwest Regional Telehealth Resource Center (MT, WA, AK, OR, ID, UT, WY)
www.nrtrc.org

Pacific Basin Telehealth Resource Center (HI, Pacific Basin)
www.pbtrc.org

South Central Telehealth Resource Center (AR, MS, TN)
www.learntelehealth.org

Southeast Telehealth Resource Center (GA, SC, FL, AL)
www.setrc.us

Southwest Telehealth Resource Center (AZ, CO, NM, NV, UT)
www.southwesttrc.org

TexLa Telehealth Resource Center (TX, LA)
www.texlatrc.org

Upper Midwest Telehealth Resource Center (IN, IL, MI, OH)
www.umtrc.org

HIPAA and Telehealth

Compliance with the Health Insurance Portability and Accountability Act (HIPAA) is more complex than simply using products that claim to be "HIPAA-compliant." HIPAA compliance entails an organized set of secure, monitored, and documented practices within and between covered entities. Though products cannot ensure compliance, some products may contain elements or features that allow them to be operated in a HIPAA-compliant way.

Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), enacted August 21, 1996, protects personal health information (PHI). In 2000, the US Department of Health and Human Services (HHS) finalized the "Privacy Rule," (with modifications made in 2002) which addressed the use and disclosure of individuals' health information, and provides standards for individuals' privacy rights under HIPAA. The Health Information Technology for Economic Clinical Health (HITECH) Act of 2009 created or further clarified provisions that impacted HIPAA.

Only certain parties, called "covered entities," are subject to HIPAA. These entities include:

- **Health plans**;
- **Health care providers**;
- **Health care clearing houses**;
- **Business associates**, defined as an entity that:
  - Creates, receives, maintains, or transmits protected health information to perform certain functions or activities on behalf of a covered entity;
  - Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to, or for, a covered entity in situations where PHI is involved;
  - Provides data transmission services to a covered entity and has access to PHI on a routine basis;
  - Offers personal health records to one or more individuals on behalf of a covered entity;
  - Operates as a subcontractor of the business associate who has been delegated a function, activity, or service in a capacity other than as a member of the business associate's workforce.

Telehealth provision or use does not alter a covered entity's obligations under HIPAA, nor does HIPAA contain any special section devoted to telehealth. Therefore, if a covered entity utilizes telehealth that involves PHI, the entity must meet the same HIPAA requirements that it would for a service provided in person. The entity will need to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to PHI confidentiality, integrity and availability.[1] While some specifications exist, each entity must assess what are reasonable and appropriate security measures for their situation.

Use of specific telehealth equipment or technology cannot ensure that an entity is "HIPAA-compliant" because HIPAA addresses more than features or technical specifications. Nevertheless, certain features may help a covered entity meet its compliance obligations. For example, a telehealth software program may contain an encryption feature, or the technology might provide security through the use of required passwords. However, these examples only provide elements or tools to help a covered entity meet its obligations under HIPAA; they do not ensure compliance, and cannot substitute for an organized, documented set of security practices.

Wireless

One common question that arises with telehealth is the appropriate mode of connectivity to transmit the PHI. For example, how secure should a wireless connection be? Regulations state that for 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."[2] A covered entity would need to assess what would be appropriate to meet such a requirement.

Business Associates

Further complications may arise in determining who would be considered a "business associate" for telehealth services, and therefore required to enter a business associate agreement in order to maintain the covered entity's compliance. For example, web conferencing services like Skype and Face Time have been used as platforms to provide clinical telehealth services, and questions may arise regarding these companies' HIPAA-related obligations. In 2011, Skype issued the following statement:

> ***Skype is not a business associate subject to HIPAA, nor have we entered into any contractual arrangements with covered entities to create HIPAA-compliant privacy and security obligations. Instead, Skype is merely a conduit for transporting information, much like the electronic equivalent of the US Postal Service or a private courier. Skype does not use or access the protected health information (PHI) transmitted using our software. However, Skype has implemented a variety of physical, technical and administrative safeguards (including encryption techniques) aimed at protecting the confidentiality and security of the PHI that may be transmitted using Skype's calling and video calling products.*** **~ Harvey Grasty[3]**

The HITECH Act clarified the definition of a "conduit". A conduit is narrowly defined as an entity that transports information, but does not access it except on a random or infrequent basis as necessary to perform the transportation services. Entities claiming exceptions as a conduit will need to meet this narrow definition, and it will be fact-specific based on the nature of the services provided, and the extent to which the entity needs to access the PHI.

While an organization may not be a "business associate" required to meet HIPAA requirements, it is unclear whether a covered entity meets HIPAA requirements by utilizing that organization. For example, under HIPAA a covered entity is required to "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking systems."[4] Will an organization like Skype allow a covered entity to meet its obligation under HIPAA? A covered entity must examine if the technology or outlet used for telehealth enables the entity to meet HIPAA's requirements.

State Law

Where state law or regulation is contrary to HIPAA, the federal law or regulation will generally prevail. However, there are some exceptions, such as cases where state law provides greater privacy protection than what is required federally. Some states have taken action to implement more aggressive laws pertaining to PHI. An entity must also keep state health information privacy and security laws in mind when developing a telehealth program.

Resources

- HIPAA Federal Regulation Codes – 45 CFR Parts 160, 162, & 164 • **www.hhs.gov/ocr/privacy/hipaa/administrative/combined/**
- National Institute of Standards & Technology • **www.nist.gov/healthcare/**
- Office of the National Coordinator • **www.healthit.gov/**
- US Department of Health & Human Services • **www.hhs.gov/ocr/privacy/index.html**

Disclaimer: This paper should not be construed as legal advice. Always consult with legal counsel.

[1] **§ 164.308 Administrative Safeguards.**
[2] **§ 164.312(e)(1) Technical Safeguards.**
[3] **Skype Statement, March 2011. onlinetherapyinstitute.com/2011/03/videoconferencing-secure-encrypted-hipaa-compliant/**
[4] **§ 164.308(a)(1)(ii)(D) Administrative Safeguards**