VOIP for Telerehabilitation: A Risk Analysis for Privacy, Security, and HIPAA Compliance

Valerie J.M. Watzlaf, PhD, RHIA, FAHIMA, Sohrab Moeini, MS, and Patti Firouzan, MS, RHIA
Department of Health Information Management, School of Health and Rehabilitation Sciences, University of Pittsburgh, Pittsburgh, PA

Abstract

Voice over the Internet Protocol (VoIP) systems such as Adobe ConnectNow, Skype, ooVoo, etc. may include the use of software applications for telerehabilitation (TR) therapy that can provide voice and video teleconferencing between patients and therapists. Privacy and security applications as well as HIPAA compliance within these protocols have been questioned by information technologists, providers of care and other health care entities. This paper develops a privacy and security checklist that can be used within a VoIP system to determine if it meets privacy and security procedures and whether it is HIPAA compliant. Based on this analysis, specific HIPAA criteria that therapists and health care facilities should follow are outlined and discussed, and therapists must weigh the risks and benefits when deciding to use VoIP software for TR.

Keywords: Risk analysis, Voice over the Internet Protocol (VOIP), telerehabilitation, HIPAA, privacy, security

Introduction

Voice over the Internet Protocol or VoIP technologies are used for more than just talking long distance to family members in another city or country. VoIP can take on several different forms including telephone handsets, conferencing units, and mobile units (Kuhn, Walsh, & Fries, 2005). Some of these software systems are used by health care providers to provide telemedicine, telepsychiatry, and TR services to patients via voice and video teleconferencing. According to the National Institute of Standards and Technology (VoIP 800-58) the main advantages of VoIP are its cost and integration with other services such as video across the Internet which then provides a teleconferencing system. Most VoIP systems are cheaper to operate than an office telephone or teleconferencing system. The disadvantages of VoIP are the start-up costs and security. Since VoIP is connected to the data network and may share some of the same hardware and software, there are more ways for the data to be compromised, so increased security on a VoIP system may be necessary. Most VoIP technology systems provide a very reliable, high quality and competent teleconferencing session with their patients. However, to determine if the VoIP videoconferencing technologies are private, secure and compliant with the Health Insurance Portability and Accountability Act (HIPAA), a risk analysis should be performed. This paper will provide a description of risk analysis issues as well as a HIPAA compliance checklist that should be used for VoIP software systems that may be used in the TR setting.

Background of Hipaa Privacy and Security Regulations and Hitech

The Health Insurance Portability and Accountability Act (HIPAA) implemented in 1996 encompasses a number of different provisions related to health insurance coverage, and electronic data exchange, along with provisions that address security and privacy of health data. Recent revisions were enacted as part of the American Recovery and Reinvestment Act of 2009, and address the privacy and security concerns associated with the electronic transmission of health information under the HITECH Act (Health Information Technology for Economic and Clinical Health Act) (Lazzarotti, 2009).

The Privacy Rule, which took effect in April 2003, established regulations for the use and disclosure of Protected Health Information (PHI), and set into play a number of sections that outline an individual's privacy rights with regard to PHI, and the expectations set forth for health care organizations and providers in ensuring

that those rights are upheld.

The Security Rule, also implemented in April 2003, outlines three types of security measures that must be taken in order to comply with the privacy rule regulations and deals specifically with Electronic Protected Health Information (EPHI). These measures include administrative, physical and technical safeguards that should be administered as part of the security rule.

The HITECH Act revisions require increases in civil penalties for different categories of violations and penalties will apply even where the covered entity did not know (and with the exercise of reasonable diligence would not have known) of the violation.

Information Security Risks:

There are three types of information security risks: Confidentiality, Integrity, and Availability. Confidentiality refers to the need to keep information secure and private. Integrity refers to information remaining unaltered by unauthorized users. Availability includes making information and services available for use when necessary. According to the NIST SP 800-58, there are many places in a network, for intruders to attack. Intrusions may also occur when VoIP telephone is restarted or added to the network

The vulnerabilities described by NIST in their report on VoIP technologies are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in many VoIP systems (Kuhn, Walsh, & Fries, 2005).

HIPAA Compliance Checklist

A HIPAA compliance checklist, specific to VoIP videoconferencing used between patients and therapists to provide TR therapy, is included so that therapists and health care facilities can take any VoIP software system they are thinking of using and determine if it meets basic privacy and security provisions. Every potential user (therapist or healthcare facility) should review the privacy and security policies that are found on the VoIP software system's website to determine if they answer the questions listed in this checklist. If the question is not addressed in the policy, then the user may want to contact the software company and ask them how the company will address a particular question(s). Then the user can determine whether the question(s) that are not answered outweigh the benefits of using a VoIP videoconferencing system to provide TR therapy to their patients.

HIPAA Compliance Checklist for VoIP (Videoconferencing) between Patients and Therapists			
PRIVACY	Yes	No	Not included in policy
1. Personal Information • Will employees and other users of VoIP software be able to listen in to video-therapy calls between patient and therapist?			
• Will video-therapy content of sessions between the therapist and patient be accessible to individuals within (employees) and outside of the software organization (other users/consumers)?			
• Will video-therapy content be shared further to protect the company's legal requirements, interests, enforce policies or to protect anyone's rights, property or safety?			
• Will video-therapy content be shared with distributors of the software or with analytical services or banking organizations etc.?			
• Will the VoIP software company provide the user 30-60 days to comply with a new privacy policy, if it has changed?			
• Will the user be able to amend personal information within a reasonable period of time and upon verification of their identity?			
• Can a user's contact see that they are online and choose to send them an email during a video conferencing session?			
RETENTION OF PERSONAL INFORMATION			
• Are video conferencing sessions for TR therapy services recorded?			
• Will video conferencing TR therapy sessions be retained and for how long?			
• How long will other personal information be retained and what will this include?			

• If a patient requests that past information be deleted, does the privacy policy state how this will occur?			
• Is the level of access (management) of the TR videoconferencing recording up to the user?			
• Does the user get the option of archiving their records offline on storage network devices?			
2. Voicemail: • Will voicemail for another VoIP user be transferred to a third party service provider?			
• If a third party service provider is used to convert and analyze the voicemail, is the background and training of the third party provided?			
• Does the background include training related to privacy and confidentiality issues related to HIPAA and other privacy statutes?			
3. Requests for Information from Legal Authorities etc. • Will personal information, communications content, and/or traffic data when requested by legal authorities be provided by the VoIP software company?			
• Is information on the educational backgrounds and experience of employees working at the VoIP software company who will decipher these requests provided?			
• Will a qualified individual who is a Registered Health Information Administrator (RHIA) with privacy, confidentiality, and HIPAA compliance experience analyze these requests?			
• Will a complete and accurate consent to patient disclosure be made?			
• Will appropriate processing of the personal data that is necessary to meet a valid request be made?			

• Will a subpoena or court order be requested from law enforcement and government officials requesting personal information?			
• Will an accounting of disclosures be made and provided to the user?			
• Are patients able to request a restriction of uses and disclosures?			
4. Sharing of Personal Information in Other Countries • Will a transfer of personal information outside of your country to a third party be made by the VoIP software company?			
• Will the use of any VoIP products automatically consent to the transfer of personal information outside of your country?			
• Since privacy and confidentiality regulations change across different countries, how will different countries maintain personal health related data and video?			
• Will other countries who may not abide by the HIPAA requirements, have the opportunity to release personal information more easily and without regard for legal requirements?			
• Should personal information that is acquired during video conferencing be transferred to a third party that the software company may buy or sell as part of its business agreements?			
• Should the patient have the right to consent to this transfer of personal information?			
• If the patient consents, with how many different countries will their personal information be shared, when participating in TR video conferencing therapy?			

5. Linkage to Other Websites: • Will the VoIP software contain links to other websites that may have a different privacy policy than their policy?			
• Does the VoIP software company accept responsibility or liability for these other websites?			
• Is the VoIP considered a business associate with the tele-therapy site being the covered entity?			
• Will the covered entity need to have business associate agreements with each of the other websites in which personal information may travel?			
• Will the other websites need to comply with privacy and security (HIPAA) requirements on their own?			
• How will the VoIP software company handle privacy and security protections under the HITECH amendment of HIPAA rules?			
SECURITY			
6. Encryption: • Are voice, video, and instant message conversations encrypted with strong encryption algorithms that are secure and private during transmission?			
• Does the encryption protect video TR therapy sessions from potential eavesdropping by third parties during transmission?			
• Does the encryption implementation contain specific information to explain what it entails?			
• Can third parties be able to decode a recorded VoIP video and voice conversation by accessing encryption keys?			

7. Anti-Spyware and Anti-Virus Protection: • Is it the user's responsibility to make sure that appropriate anti-virus and anti-spyware protection is on their computer in order to prevent eavesdropping during videoconferencing TR sessions?			
• How secure are videoconferencing TR sessions and how much personal health information may be transmitted to other authorities?			
• Are patients informed of the security issues and is this included in their informed consent?			
8. User's Public Profile: • Is it *optional* for the user to enter information into their public profile			
• Is the user *required* to enter any information into the public profile?			
• If the public profile information be seen by other users can the user determine which information can be seen by whom?			
• Is the public profile separated into the following three categories? 1. Information that *everyone* can see.[1] 2. Information for *only the user's contacts* to see.[1] 3. Information for *no one* to see.[1]			
• Is the user's email address encrypted so *no one* can see it when looking at the profile?			
• Are there instructions on how users can update and change the profile information?			

[1] *As per Skype Privacy Policy, http://wwwskype.com retrieved August 15, 2010*

9. Allowing, Removing, Blocking Callers: • Does the VoIP software system allow the user to determine if they want to contact a person in their contact list?			
• Are contacts easily removed by the user?			
• Can the user remove or revoke authorization by blocking the user on each computer that is used?			
• Does the VoIP software system provide instructions on how to block a user?			
10. Audit System Activity: • Are server logs generated to provide a record of the compliance settings that the user developed?			
• Do the logs also provide an audit trail to track who had access to TR videoconferencing sessions and which functions were enabled or disabled for the session?			
11. Security Evaluation: • Has a security evaluation of the VoIP software system been performed by an independent group?			
• Does the security evaluation include authentication, password management, data management etc. and verifies that the software system implements proper security measures?			

VoIP Risks and Recommendations:

The risks, threats and vulnerabilities related to a VoIP as explained by NIST are described below with recommendations on how these can be reduced or eliminated. This list is not exhaustive as some of the VoIP systems may have privacy and security risks that are not included below. However, it does provide information as to where a risk may occur, the level of risk and a recommendation on how to prevent the risk from occurring (Kuhn, Walsh, & Fries, 2005).

Risk, Vulnerability or Threat	Specific Area	Risk Level	Recommendation
1. Confidentiality and Privacy	Retention of personal data and information as well as eavesdropping on conversations.	High (increases in VoIP because of the many nodes in a packet network)	Change default passwords; disable remote access to graphical user interface; use authentication mechanisms.
	System vulnerabilities: viruses, worms, Trojans	High	Implement VLAN with stand alone workstation, separate from user workstation. Separate "softphone" applications from regular software applications.
	IP (Internet Protocol) Packet Transmission	High	Outside of the network environment, proper encryption protocols such as IPsec should be incorporated when transmitting data. IPSec uses proper authentication and encryption protocols when communicating and transmitting data.
	Wiretap vulnerability/ intercept voice traffic	High (attaching a packet capture tool to the VOIP network segment increases changes to intercept voice traffic)	Establish a good physical security policy; develop an alarm system to notify administrator when an IP phone is disconnected; use authentication mechanisms. Preferably use a wired network over WiFi alternatives.

	Web server interfaces used to gain confidential information	High	Use the more secure web server if it is necessary to use it for remote administration.
	IP address extension leads to other attacks of confidential information	High	Disable the IP phone; it is very simple to turn it back on once an attack is prevented.
2. Integrity Issues	Legitimate user may perform incorrect or unauthorized function which may be due to a level of access given to the user that is higher than needed.	High	Provide the user with a level of access that is appropriate to their need. (For example, do not provide users to gain access to personal health information if it is not necessary for their level of work.)
	Intruder acting like a legitimate user	High	Use IP phone instruments that can download signed binary files by users.
	Insecure state of the switch (switch is a small hardware device that joins multiple computers together within one local area network)	High	Firewalls, change default passwords, disable graphical user interface. Disable port mirroring and port forwarding and implement VoIP aware firewalls.
3. Availability of Service	Flooding the link with bogus messages causing severe deterioration or denial of service or functionality	High (VOIP may have additional vulnerabilities with Internet connection)	Deploy a firewall that eliminates connections from unnecessary or unknown networks; change default passwords and disable graphical interface; check software updates; limit login attempts until account becomes locked out.

Overall Recommendations:

Whatever software application is chosen to be used for TR videoconferencing therapy, each therapist and health care entity should consider implementing the following recommendations before its use:

- Form a team of health and legal professionals that will examine VoIP software systems to determine if it meets federal (HIPAA), state, local, and facility-wide privacy and security regulations. Since VoIP software systems can change frequently, a team of professionals is needed to stay up-to-date on those changes. Also, federal and state policies change frequently, so again the team must ensure that someone is on top of these changes. The team may consist of the health care facility attorney, risk management personnel, health information administrator/ privacy officer, security officer (IT) and representative therapists (e.g., occupational therapist, physical therapist and speech-language pathologist).
- Educate and train therapists and other rehabilitation personnel who use TR software applications for video conferencing on all aspects of privacy and security issues related to video conferencing as well as exchange of other PHI. Awareness training on all aspects of HIPAA security rules in relation to TR and software use, spyware, password security, and encryption should be emphasized in relation to video conferencing. Education and training should emphasize what therapists should look for when considering use of certain software applications for video therapy in relation to privacy and security as well as quality and reliability. Many times the privacy and security of a system is overlooked because of how well it can provide a TR service.
- Develop an informed consent form that patients sign that explains the TR therapy that will be provided, how the VoIP technology software will be used and why, the benefits of the TR and use of video conferencing communication, as well as the risks related to privacy and security. Have the team attorney review the informed consent to make sure it meets all federal (HIPAA), state and local regulations.
- Incident response is necessary and should include documentation regarding the incident, the response to the incident, any effects of the incident as well as whether policies and procedures that were followed in response to the incident. If policies and procedures are not in place for incident response, then these should be developed with the security and privacy officers.
- Use the HIPAA compliance checklist and compare it to the VoIP technology software privacy and security policies. Or, purchase HIPAA compliance software specific to VoIP that will walk you through each piece of the HIPAA legislation to make certain the software is private and secure.
- Consider the future of using VoIP technology software if the HIPAA regulations change to include them as business associates or if stronger recommendations are made for VoIP software technology, since the DHHS is also looking more closely at entities that are not covered by HIPAA rules to understand better how they handle PHI and to determine whether additional privacy and security protections are needed for these entities.
- Follow all applicable security safeguards when using VoIP, such as those recommended by the NIST (Kuhn, Walsh, & Fries, 2005) and Garfinkel (2005). These include not using the username and password for anything else but video conferencing, changing it frequently and not making it easy to identify; not having computer viruses on the computer used for video conferencing; never use it for emergency services; and consistently authenticate who you are communicating with especially when used for tele-therapy video sessions.
- Provide audit controls for using software applications so that they are secure and private. Focus on the transmission of data through video conferencing, how that data is made private and secure during the telecommunication, and also how private and secure it is stored and released to internal and outside entities.
-

References

Centers for Medicare and Medicaid Services, HIPAA General Information. Retrieved September 9, 2010 from http://www.cms.gov/HIPAAGenInfo/.

Garfinkel, S. (2005). VoIP and Skype security. Skype Security Overview-Rev 1.6 Retrieved July 11, 2010 from http://www.tacticaltech.org/files/tacticaltech/Skype_Security.pdf.

Kuhn, D., Walsh T., & Fries S., (2005). Security considerations for voice over IP systems: Recommendations of the National Institute of Standards and Technology (NIST). Technology Administration, U.S. Department of Commerce Special Publication, 800-58.

Lazzarotti, J., HIPAA Enforcement Regulations Updated for Penalty Increases and Enhancements under the HITECH Act, Retrieved September 9, 2010 from http://www.workplaceprivacyreport.com/2009/11/articles/hipaa-1/hipaa-enforcement-regulations-updated-for-penalty-increases-and-enhancements-under-the-hitech-act/.