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

Valerie J.M. Watzlaf, PhD, RHIA, Fahima, Sohrab Moeini, MS, Laura Matusow, BS, RHIA and Patti Firouzan, MS, RHIA.
Department of Health Information Management, School of Health and Rehabilitation Sciences, University of Pittsburgh, Pittsburgh, Pa.

Abstract

In a previous publication the authors developed a privacy and security checklist to evaluate Voice over Internet Protocol (VoIP) videoconferencing software used between patients and therapists to provide telerehabilitation (TR) therapy. In this paper, the privacy and security checklist that was previously developed is used to perform a risk analysis of the top ten VoIP videoconferencing software to determine if their policies provide answers to the privacy and security checklist. Sixty percent of the companies claimed they do not listen into video-therapy calls unless maintenance is needed. Only 50% of the companies assessed use some form of encryption, and some did not specify what type of encryption was used. Seventy percent of the companies assessed did not specify any form of auditing on their servers. Statistically significant differences across company websites were found for sharing information outside of the country (p=0.010), encryption (p=0.006), and security evaluation (p=0.005). Healthcare providers considering use of VoIP software for TR services may consider using this privacy and security checklist before deciding to incorporate a VoIP software system for TR. Other videoconferencing software that is specific for TR with strong encryption, good access controls, and hardware that meets privacy and security standards should be considered for use with TR.

Keywords: Voice over Internet Protocol (VOIP), telerehabilitation, HIPAA, privacy, security, evaluation

Introduction

Voice over Internet Protocol (VoIP) videoconferencing software is sometimes used to provide telerehabilitation therapy (TR). VoIP software systems enable a healthcare provider to offer TR services to clients who may not be able to access their services in the office setting. This can be quite advantageous for the client and therapist. Before healthcare providers embark on the use of VoIP, they should first consider whether patient correspondence, through video, voice and any other health information that may be released via the VoIP system will be kept private and secure and will meet HIPAA requirements.

Background

There is much uncertainty that exists between healthcare providers, information technology experts, health care facilities, and malpractice carriers as to whether VoIP is private, secure, and HIPAA compliant. There is also confusion over whether VoIP systems like Skype, Google Talk and others are considered business associates and therefore must meet the new HIPAA requirements under the HITECH Act. Some health care providers have used VoIP in research studies when testing certain TR services to patients who live in remote or rural areas or who are unable to travel into the office for treatment (Herman et al. 2010; Cason, 2009).

Some health care providers use VoIP for very private and confidential purposes such as tele-psychiatry and believe it provides an important service for rural mental health patients at a low cost, while eliminating travel time and office wait times (Skype Business Blog, 2009). Still others in tele-psychiatry not only use VoIP but believe some systems are HIPAA compliant (http://voyagerllc.blogspot.com/2009/06/skype-and-hipaa-myth-buster.html).

However, other psychotherapists do not believe that VoIP should be used for tele-psychiatry and state that it is not secure, confidential or HIPAA compliant (Zur, 2010; Maheu, 2009a; Maheu, 2009b). The Campania Group is one malpractice carrier that offers support for home-based tele-psychiatry (Ikelheimer, 2008).

Some health information technology (HIT) experts believe VoIP is not as secure as its security policies describe and that telecommunication via video and voice

calls may not be fully secure even though encryption is used. This is mainly because there is not enough information within some of the VoIP security policies to detail how the encryption works, and when experts don't know how it works they tend to be more skeptical (Lazar, 2006, Garfinkel, 2005, MIT, 2008)]. Some of these same HIT experts also believe that although VoIP has security issues, it may be best to weigh the advantages against the disadvantages when deciding to use it for video conferencing with clients (Lazar, 2006; Garfinkel 2005).

The US Army uses mCare, a mobile technology for appointment reminders and other health care tips to support wounded soldiers, particularly, traumatic brain injury soldiers, and states that the mCare system is HIPAA compliant. Even though this system is different than VoIP systems, since it includes only mobile technology, it is the Army's preferred telecommunication system and meets both privacy and security regulations (Lewis, 2010).

The Department of Health and Human Services, Office for Civil Rights have modified the HIPAA Privacy, Security and Enforcement rules which fall under subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH), Title XIII of the American Recovery and Reinvestment Act (ARRA) of 2009. The proposed rule includes an expansion of what encompasses a "business associate." A business associate, according to HIPAA includes any entity that works on behalf of the covered entity and handles protected health information (PHI). Is a VoIP videoconferencing software system that is used for TR considered a business associate of a covered entity if the covered entity is the healthcare system? If so, the covered entity or healthcare facility would then need to enter into a business associate agreement with the VoIP company and will need to have systems in place to meet the new and existing HIPAA privacy and security regulations. However, it is unclear whether VoIP systems are business associates. It would seem that most VoIP software systems would fall under this definition. Other provisions include prevention of breaches of healthcare information and also the obligation to notify clients quickly when a breach occurs. The definition of breach under the new provisions means the unauthorized acquisition, access, use or disclosure of PHI, which compromises the security or privacy of such information. The new amendments also restrict the sale of health information; provide new access rights for obtaining healthcare information in electronic format; and impose new and increased penalties with the enforcement and improvement of the Privacy Rule (Callahan, 2010).

VoIP systems and the entities that use them for TR purposes will need to comply with the new HIPAA provisions if VoIP is considered a business associate, because these new provisions include business associates directly. Therefore, it is important for private practices and health care facilities that use VoIP systems to address and comply with the privacy and security guidelines and HIPAA requirements.

HIPAA Compliance Checklist

A HIPAA compliance checklist (Watzlaf, Moeini, & Firouzan, 2010) was developed to assist therapists and health care facilities in assessing a VoIP software system. Every potential user (e.g., independent practice 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.

Objectives

The objectives of this study were to:

1. Gain knowledge about the privacy and security policies of VoIP software systems.
2. Understand the risks and benefits involved with VoIP software systems.
3. Perform a risk analysis on VoIP software systems to determine compliance with privacy and security issues.
4. Provide recommendations to healthcare providers and clients when using VoIP for TR.

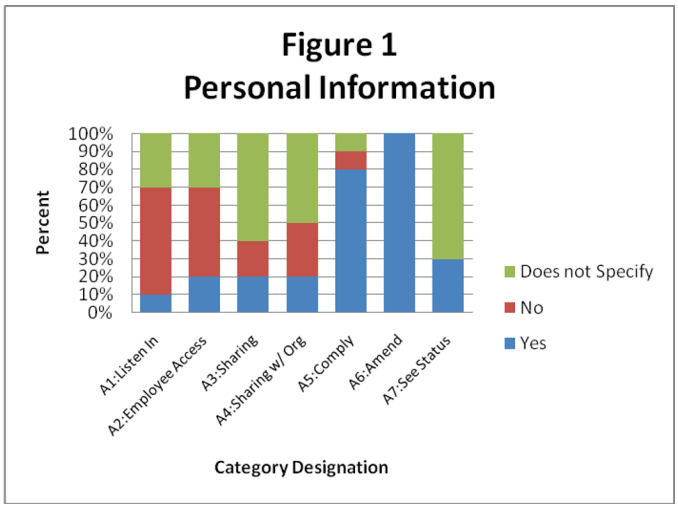
A review and analysis of the privacy and security policies of the top ten VoIP software companies will provide a first step in determining how well VoIP software systems are addressing privacy and security issues related to the use of VoIP with TR.

Methodology

A risk analysis of the ten most popular VoIP videoconferencing software systems was performed to determine if their privacy and security policies or their terms of use addressed the HIPAA compliance checklist. The top sites were selected from two different websites that reviewed VoIP software systems. Each website of the ten VoIP companies and each privacy and/or security policy and/or terms of use, whichever was available on the site, was reviewed and analyzed for each of the 58 questions listed in the checklist. Also, each site was contacted via email if there were some questions that could not be answered from the information on their website. A Health Information Management student performed the initial review of each of the VoIP websites in comparison to the checklist. A second review of 20 percent of the VoIP companies was performed by the

same HIM student with 100% percent agreement. A doctoral student in Health Information Systems with 5 years of health information technology experience performed a sample audit of 40% percent of the systems reviewed initially with 100% percent agreement. The primary author performed a sample audit of 20% percent of the previous two reviews with 100% percent agreement. A summary of the results of the assessment are provided below.

Results



The first seven questions of the compliance checklist focus on whether a VoIP company's video-therapy content can be accessed by employees within or outside of the company. It can be seen from Figure 1 that 60% of the companies claim that they do not listen into video-therapy calls unless maintenance is needed. However, one company can see account details and details about the conversation between users. One company that can listen into the video-therapy call stipulates that it is only for service problems and they must have the consent of the user. However, for the other 30%, it could not be determined from their policies whether they could listen in. As to whether video-therapy content is accessible to employees and other users, 50% of the VoIP companies said no; 10% said yes, it is a possibility; and 30% did not specify. As far as sharing of the video-therapy content (Figure 1: A3 & A4), 60% and 50% respectively, did not specify this in their policies. A 30-60 day period for compliance with a new privacy policy if it has changed, received a high compliance score of 80%. All of the VoIP companies allow amending of personal information within a reasonable period of time. Seventy percent do not specify in their privacy and security policies whether a user's contacts can see their status and choose to send them an email during a video-conferencing session. A Chi square statistic was calculated and it was found that there is no significant difference across VoIP companies for questions related to personal privacy information (p=0.254).

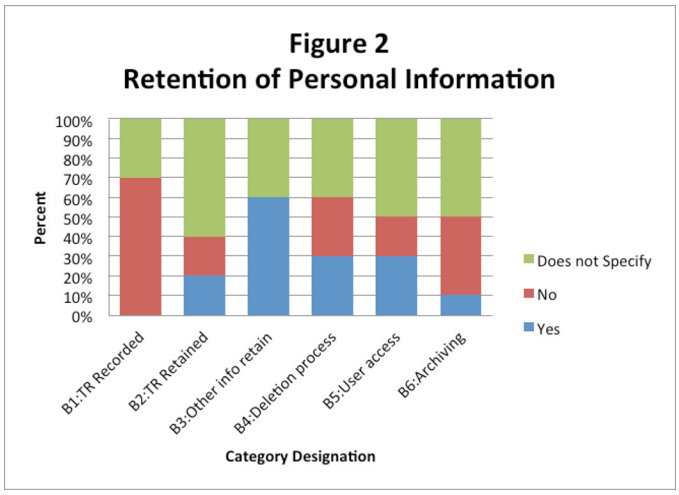
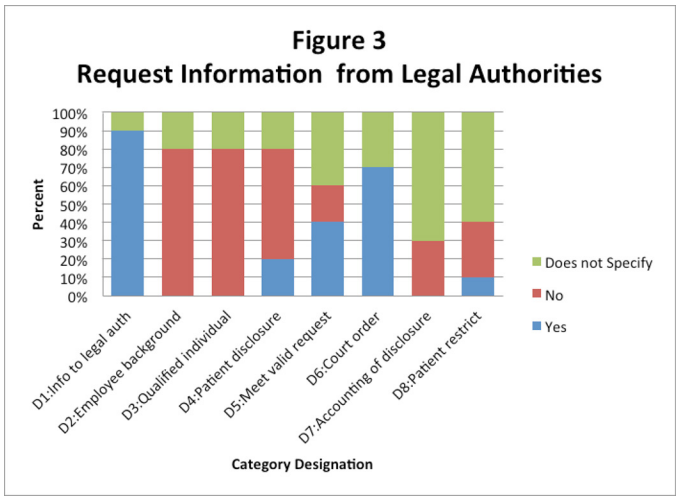
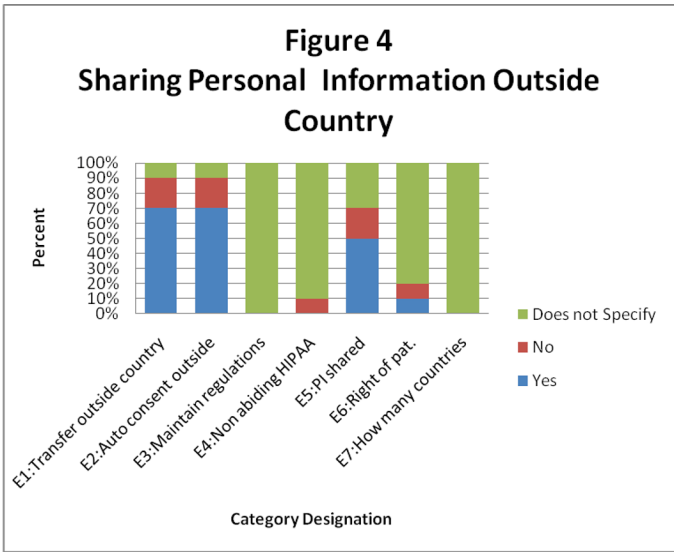


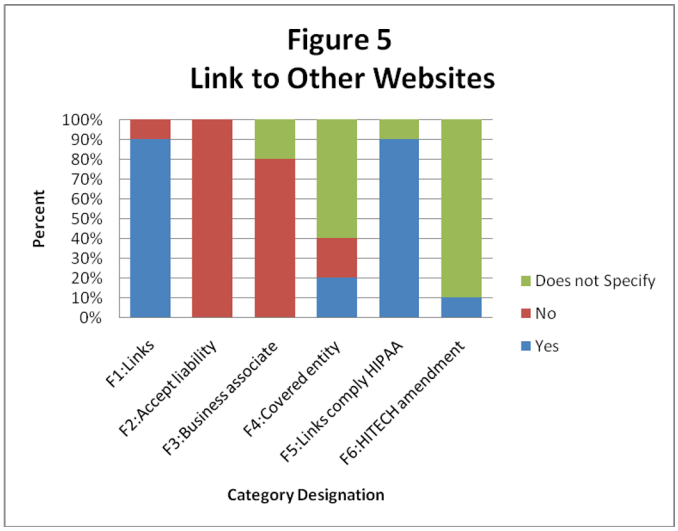
Figure 2 addresses retention of personal information such as whether the TR therapy session will be recorded and retained and for how long. Seventy percent of the companies indicate they do not record the TR therapy sessions, while 30% do not specify this information in their policies. However, one company offered that users have the option to save their video sessions on their own computers and another stated that there is a recording solution and sessions are stored on the server for 30 days but not viewed by anyone. Other personal information is retained by 60% of the companies, and deletion of past information by the user is available for 30% of the companies. Thirty percent allow the user to access and manage the TR session. Only 10% of the companies allow the user to archive their records offline on storage network devices. A Chi Square statistic was calculated and it was found that there is no significant difference across VoIP companies for questions related to retention of personal information (p=0.112).



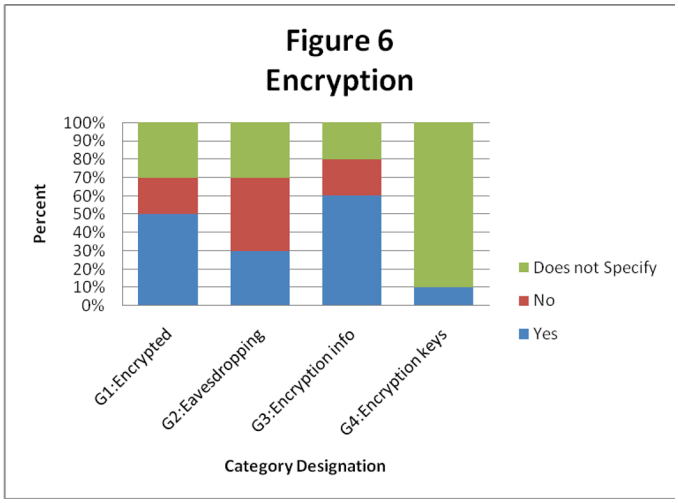
Ninety percent of the VoIP company policies state that personal information, communications content, and/or traffic data will be provided to legal authorities when requested (Figure 3). Eighty percent of the companies do not provide backgrounds on the employees who would be deciphering these requests, and do not indicate that they have a qualified individual with privacy and security experience analyze these requests. Also, only 20% of the companies state that a complete and accurate consent to patient disclosure will be made, while 30% state that an accounting of disclosures will be made and provided to the user, and users are able to request a restriction of uses and disclosures. A Chi Square statistic was calculated and it was found that there is no significant difference across VoIP companies for questions related to requests for information from legal authorities (p=0.224).



Some of the VoIP companies reviewed are based outside of the United States and the software is freely available on the Internet. This brings up various concerns regarding the possibility of data storage outside of the US and the HIPAA implications this may have. It can be seen from Figure 4 that 70% of the companies will allow a transfer of information outside of the country to a third party. This is problematic, because the use of VoIP products automatically provides consent to this transfer of personal information. None of the companies stated how different countries will maintain the confidentiality of personal health data and only 10% stated that companies in other countries do not release information more easily than in the US, even though they do not have to abide by HIPAA. Fifty percent of the companies will share personal information acquired during video conferencing to a third party that the company may buy or sell as part of its business agreements. Also, only 10% allowed the user to consent to a transfer of personal information. None of the companies specified how many different countries the personal information could be shared with. A Chi Square statistic was calculated and it was found that there is a significant difference across VoIP companies for questions related to sharing of personal information outside of the country of origin (p=0.010).



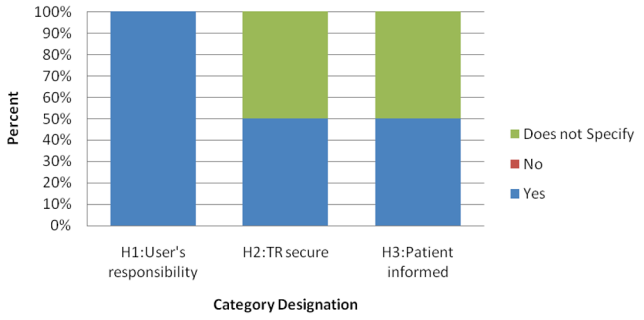
It can be seen from Figure 5 that 90% of the VoIP companies do contain links to other websites that may have a different privacy and security policy than their own and none of the companies accept responsibility or liability for these other websites. Ninety percent of the companies state that the other websites will need to comply with privacy and security requirements on their own and they did not specify how they will handle changes that may come about due to the HIPAA amendments. A Chi Square statistic was calculated and it was found that there is no significant difference across VoIP companies for questions related to linkage to other websites (p=0.980).



The security of a VoIP system is extremely important, especially when the system is used for TR. Encryption

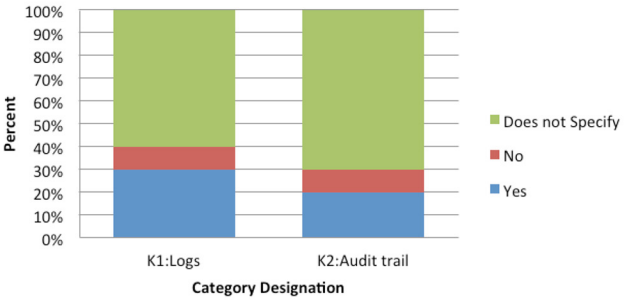
is the ability to transform data using specific algorithms so that the information is unreadable to anyone, other than those who have access to the encryption keys. Encryption can be used on everything from personal data on a server to data being transmitted via video and audio. For example, employing at least a 128-bit Advanced Encryption Standard (AES) over SRTP (Secure Real-time Transport Protocol) for video and audio transmissions is recommended. The National Institute of Standards and Technology (NIST) also recommends AES over Data Encryption Standard (DES) in certain protocols such as Session Initiation Protocol (SIP), (Kuhn, Walsh & Fries, 2005). However, only 50% of the companies assessed use some form of encryption (Figure 6). Also, only 30% said that their encryption could protect against eavesdropping by third parties. Some companies that use encryption did not specify what type of encryption is used. A Chi Square statistic was calculated and it was found that there is a significant difference across VoIP companies for questions related to encryption (p=0.006).

Figure 7
Anti-Virus Protection



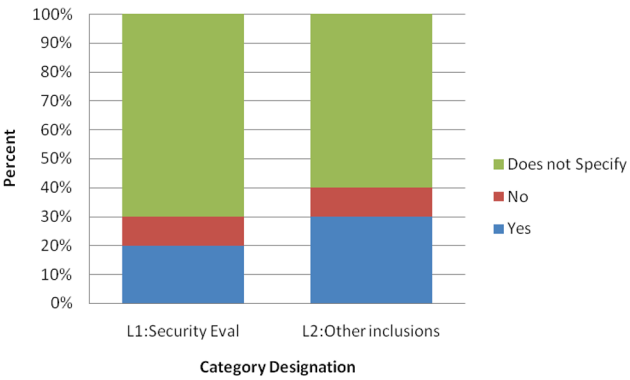
All of the VoIP companies state that it is the user's responsibility to provide appropriate anti-virus and anti-spyware protection on their computer in order to prevent eavesdropping during a videoconferencing session (Figure 7). Fifty percent of the companies address whether the videoconferencing session is secure but only 40% use encryption to enable this security. Also, 50% of the VoIP companies state in their policies that users are informed of any security issues. A Chi Square statistic was calculated and it was found that there is no significant difference across VoIP companies for questions related to anti-virus protection (p=0.437).

Figure 8
Security: Audit System



Thirty percent of the companies said that they have some form of auditing, through logs (Figure 8). Twenty percent use an audit trail. Seventy percent of the companies assessed did not specify any form of auditing. A Chi Square statistic was calculated and it was found that there is no significant difference across VoIP companies for questions related to an audit system (p=0.182).

Figure 9
Security Evaluation



Security evaluations by an accredited independent party are a good way to assess a company's security infrastructure. Very few of the companies assessed performed security evaluations from outside companies (Figure 9). Seventy percent of the companies made no mention of a security evaluation, 20% said they have one, and 10% stated that they do not partake in such an analysis. Also, only 30% of the company's policies state that the security evaluation includes authentication, password management, data management, and so forth. A Chi Square statistic was calculated and it was found that there is a significant difference across VoIP companies for questions related to security evaluation (p=0.005).

Study Limitations

As with any study there are limitations to the study design. The privacy, security, terms of use policies and procedures, and email responses to any questions not included in the policies of the VoIP company website were reviewed and analyzed. The VoIP videoconferencing software systems were not used in order to determine how they compared to the privacy and security checklist. Also, this study was performed at one point in time, in the fall of 2010, and since that time some of the VoIP companies' websites policies may have been updated. Further review of these sites was not performed over time.

VoIP Risks vs Benefits

VoIP may pose security problems when used for a TR session. For example, if a stroke patient is online with their occupational therapist discussing a recent issue with their activities of daily living (ADLs), one of their contacts may see that they are online and choose to send them an email during this video session. This does not mean that the contact can hear the session -- but they could see that the patient is online. Based on this, will the patient believe that their personal health information is kept secure? Also, what happens to these video sessions once they are over? Are they recorded and stored, and if so, where are these recordings stored? Not knowing if the sessions are recorded is a major security issue and one that VoIP companies should address.

However, on the other side of this issue, are the claims that VoIP increases clinical productivity, patients get better faster, and costs are decreased. As one example, therapists can now use VoIP to help patients relieve their pain. In the past, therapists had distant patients videotape themselves and mail in their videotapes, with considerable lag time and expense. In contrast, current VoIP-based treatment is provided in real time. The therapist can see the patient walk across the room, observe their posture, and watch as they perform evaluative tasks, (e.g., standing on one foot) and exercises. VoIP technology allows both patient and therapist the chance to ask and answer questions immediately (Wolinsky & Titus, 2009).

Each individual therapist and health care facility will need to weigh the risks and benefits for their patients and decide whether VoIP is a private, secure and safe alternative for their patients.

Recommendations

Therapists should consider other types of VoIP that are built specifically to provide telemedicine and TR and therefore, may be more secure and private. For example, VISYTER (Versatile and Integrated System for Telerehabilitation) is a software platform that supports high quality TR videoconferencing within the home or in enterprise-wide telehealth services. It has also been used on several TR applications such as wheelchair prescription, physical therapy consults, and autistic assessments (Parmanto et al, 2010). Users of VISYTER must login in to a private server and enter a room that is restricted to the users with privilege for that room. Each user has a unique Role Based Access Control (RBAC) to connect to other users, medical information, and video-conferencing rooms. All traffic data are encrypted and there is no public ID or personal information that is accessible. Therefore, there is no information on a public site and all information will only be stored by a covered entity server, under their ISD control. VISYTER uses a 1024-bit RSA algorithm. This is used to encrypt text for authentication. Each video and audio session is encrypted using 3 DES 192 bit key. This is a private key and encrypted according to NIST standards and is valid until 2013.

Another solution to consider is VidyoHealth, designed by the Vidyo Company. VidyoHealth supports application sharing, but it does not clearly specify, to what extent, for example, it can connect to an EHR server for data exchange. VidyoHealth states that it provides security features such as:

- AES-128 bit media encryption for transmitting secure video and audio
- HIPAA compliant mobile medical carts
- HTTPS with certification login which enables a secure end to end HTTP connection with the inclusion of certification to authorize identity before usernames and passwords are sent
- Spoof prevention using rigorous authentication methods
- Leveraging the security of Linux based appliances, while at the same time closing all ports that are not relevant
- Encrypted token technology for session security (Vidyo, Inc., 2010)

It is also important that all three entities engaged in a TR transaction, (i.e., therapist, VoIP provider, and the client and/or their advocate) are cognizant of the privacy and security issues that can surround the use of a voice and video communication service when personal health information may be communicated.

Each of the three entities in a TR encounter should exercise due diligence before engaging in the use of VoIP systems for TR. If the benefits outweigh the risks for all, the VoIP system is a viable option. If not, then alternate methods of voice and video communication are needed.

Furthermore, it should not be assumed that all parties are aware of the implications and risks of using a specific VoIP system. As a condition of informed consent, there should be open communication with clients about the privacy and security issues, so that everyone involved is aware of the potential risks and benefits.

References:

1. Callahan, J.D. (2010). Privacy: The Impact of ARRA, HITECH, and other Policy Initiatives. American Health Information Management Association (AHIMA).
2. Cason, J. (2009). A pilot telerehabilitation program: Delivering early intervention services to rural families. International Journal of Telerehabilitation, 1, 29-37.
3. 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
4. Herman, V., Herzog, H., Jordan, R., Hofherr, M., Leving, P., & Page, S. (2010). Telerehabilitation and electrical stimulation: An occupation based client-centered stroke intervention. The American Journal of Occupational Therapy, 64: 73-81. http://support.mitglobalnet.net/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=9
5. Ikelheimer, D. (2008). Letters to the Editor: Treatment of opioid dependence via home-based telepsychiatry. Psychiatric Services. 59: 1218-1220. Retrieved July 10, 2010 from http://psychservices.psychiatryonline.org/cgi/reprint/59/10/1219.pdf
6. 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.
7. Lazar, I. (Speaker). (2006). Debunking the Hype about Skype [Audio Recording]. Burton Group Inflection Point.
8. Lewis, N. (2010 June 30). Army using telemedicine for healthcare delivery. Information Week: Healthcare. Retrieved on July 12, 2010 from http://www.informationweek.com/news/healthcare/patient/showArticle.jhtml?articleID=225701968
9. Magic Island Technologies. Skype. (2008) Retrieved July 12, 2010 from http://support.mitglobalnet.net/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=9
10. Maheu, M. (2009a). Comments: Is Skype HIPAA compliant? Adventures in telepsychiatry: a psychiatrist in a solo private practice experiments with telepsychiatry. Retrieved July 20, 2010 from http://adventuresintelepsychiatryblog.patrickbarta.com/2009/10/is-skype-hipaa-compliant/
11. Maheu, M. (2009b). HIPAA and hijacked Skype passwords: Another security violation that brings viability of online counseling via Skype into yet more questioning. Telehealth.Net. Retrieved July 10, 2010 from http://telehealth.net/blog/hipaa-hijacked-skype-passwords-another-security-violation-that-bring-online-counseling-to-question/
12. Parmanto, B., Saptono, A., Pramana, G., Pulantara, W., Schein, R., Schmeler, M., McCue, M., & Brienza, D. (2010). VISYTER: Versatile and Integrated System for Telerehab. Telemedicine and E-Health. 16(9):1-6.
13. Skype Business Blog. (2009). Doctors using Skype to transform medical practice. Retrieved July 9, 2010, from http://blogs.skype.com/business/2009/05/doctors_using_skype_to_transform_medical_practice.html
14. Skype and HIPAA: Myth buster. (June 6, 2009). Voyager telepsychiatry: A forum on home-based telepsychiatry. Retrieved July 9, 2010 from http://voyagerllc.blogspot.com/2009/06/skype-and-hipaa-myth-buster.html
15. Vidyo Inc. 2010, Vidyo Telepresence- Secure VidyoConferencing: Protecting Your Communications. Retrieved April 19, 2011 from VidyoInfo@vidyo.com
16. Watzlaf, V., Moeini, S., & Firouzan, P. (2010). VoIP for telerehabilitation: A risk analysis for privacy, security, and HIPAA compliance. International Journal of Telerehabilitation, 2(2), 3-14. doi: 10.5195/ijt.2010.6056
17. Wolinsky H. & Titus F. (Producer/Director), (2009). LA therapist helps clients relieve pain via Skype. YouTube Retrieved on July 12, 2010 from http://www.youtube.com/watch?v=eB5tZfZfabo
18. Zur, O. (2010). HIPAA Updates from Zur Institute: Innovative resources and online continuing education. Retrieved July 10, 2010 from http://www.zurinstitute.com/hipaa_updates.html