VoIP for Telerehabilitation: A Pilot Usability Study for HIPAA Compliance

Valerie R. Watzlaf, PhD, RHIA, FAHIMA
Briana Ondich, BS, RHIA
Department of Health Information Management, School of Health and Rehabilitation Sciences, University of Pittsburgh, Pittsburgh, PA

Abstract

Consumer-based, free Voice and video over the Internet Protocol (VoIP) software systems such as Skype and others are used by health care providers to deliver telerehabilitation and other health-related services to clients. Privacy and security applications as well as HIPAA compliance within these protocols have been questioned by practitioners, health information managers, and other healthcare entities. This pilot usability study examined whether four respondents who used the top three, free consumer-based, VoIP software systems perceived these VoIP technologies to be private, secure, and HIPAA compliant; most did not. While the pilot study limitations include the number of respondents and systems assessed, the protocol can be applied to future research and replicated for instructional purposes. Recommendations are provided for VoIP companies, providers, and clients/consumers.

Keywords: Voice over the Internet Protocol (VoIP), telerehabilitation, HIPAA

Introduction and Background Studies

Consumer-based, free VoIP systems such as Skype and others are used by some providers using a telerehabilitation service delivery model since these systems provide the use of voice and video teleconferencing between patients and therapists. Privacy, security and HIPAA compliance across these systems were evaluated in previous studies (Watzlaf, Moeini, Matusow & Firouzan, 2011; Watzlaf, Moeini, & Firouzan, 2010).

Watzlaf, Moeini, & Firouzan (2010) developed a privacy and security checklist that was used to assess consumer-based, free VoIP systems. A summary of that checklist is shown in Table 1.

Privacy and Security Parameters	Policy Affirms	Policy Denies	Policy Does Not Include
Personal information is accessible to others (e.g., via listening in; shared content; others can amend PHI)			
Retains PHI • recorded and stored? • specifies how long PHI is retained?)			
Would comply with requests for PHI from legal authorities			
Shares PHI with other countries			
Links PHI to other websites			
Shares user's public profile			
Employs anti-spyware/ virus protection			
Employs encryption			
Allows, removes, and/ or blocks callers			
Audits system activity			
Employs security evaluation			

Table 1: *Checklist for privacy and security information provided by consumer-based, free VoIP systems.*

The full 58-question checklist developed by Watzlaf, Moeini, and Firouzan, (2010) was used in a second study to assess the top ten consumer-based, VoIP systems in relation to privacy and security by examining their privacy and security policies, terms of use, and emailing the company for further information on these issues. This study demonstrated that many of these VoIP companies stated in their policies that personal information will be shared across countries, other websites, and to protect the companies' legal interests. Some privacy and security policies seemed to protect the company more than the user. For example, 90% of the companies' policies stated that personal information, communications content, and/ or traffic data will be provided to legal authorities when requested. Also, 70% of the companies allow a transfer of information outside of the country to a third party, and 90% of the companies contain links to other websites.

However, 60% of the companies claimed that they do not listen into videoconference calls unless maintenance is needed and 70% of the companies do not record the sessions, although 30% did not discuss this information in their policies. Only 50% indicated in their policies the use of encryption to protect personal information/data. Of those companies reporting the use of encryption, some did not specify what type of encryption was used. Only 30% of encryption levels used by the companies protect against eavesdropping by third parties.

Only 30% of the companies claimed they use some form of auditing (i.e., logs); 20% use an audit trail. Many companies did not discuss, in their policies, any form of auditing or audit trails on their servers. Seventy percent of the companies made no mention of a security evaluation. Because this assessment focused on the privacy and security policies and not on the actual use of the system, it was necessary to examine the privacy and security of the system in a usability study of providers simulating use of the top three, free, consumer-based VoIP systems for the delivery of therapeutic services.

Usability Study Methodology

Four respondents with graduate level education and professional certification in speech-language pathology, social work, physical therapy, and healthcare IT, were asked to use the top three, free, consumer-based VoIP systems, and answer questions similar to what was included in the privacy and security checklist. The checklist was adapted to include tasks and accompanying questions. Technical assistance was provided by the research team to the respondents as they performed the tasks and answered the questions. This study was submitted to the University of Pittsburgh Institutional Review Board and received approval at the exempt level.

Results

The tasks analyzed, accompanying questions, and results are summarized in Table 2. Taken together, the results suggest that while privacy and security for VoIP software systems are highly valued, the respondents expressed lower levels of confidence in the security and privacy of the three systems they examined.

Evaluation Parameter	User Tasks	Questions	Results
System Access	Type your user name and password upon entering the system.	Should something other than a password be used to authorize entrance into the videoconferencing system?	75 % of the respondents across all three systems responded yes to the question. Respondents indicated that additional security to access the system should be implemented (e.g., biologic data, finger print, eye scan). Respondents also indicated that a Virtual Private Network (VPN) should be utilized.
		Do you think employees of the VoIP company can listen in to the video therapy session?	83% of respondents said yes, they believe that the company can listen in to the video therapy session.
		Do you think other users can listen in to the video therapy session?	67% of respondents said yes, they believe that other users can listen in to the video therapy session
Control of Personal Information	Determine your default settings for communicating. Determine your online status. Determine how much personal information may be transmitted to others.	How would you rank the privacy and security of your default settings when conducting a video therapy session? Likert scale, 1-5 (1= not at all private and secure; 5= very private and secure)	1.9 average across all systems; respondents had low confidence in the privacy and security of the default settings.
		Do you think a user from your contact list can see that you are online and choose to send you a message?	83% of respondents across all systems said a user from their contact list could see that they were online and choose to send them a message; but, they believed that users could change the settings to prevent this (e.g., “invisible” status option).

Evaluation Parameter	User Tasks	Questions	Results
Retention of Personal Information	Determine how long your history will be kept and what it includes. Take a picture of the person you are corresponding with (via screen shot) and save it.	Do you think that video therapy sessions can be recorded by the VoIP company? Do you think that the person was aware that you took the picture? Do you think being able to take a picture is a good option to have? Rank how private you think this option is when videoconferencing with your client. Likert scale, 1-5 (1= not at all private; 5= very private)	83% of respondents indicated that they believed the video therapy session could be recorded by the VoIP company. 67% of respondents took a screen shot during a simulated therapy session and indicated that the other person was unaware that a picture had been taken. 50% of respondents indicated the capacity to take pictures is beneficial, especially to record aspects of clinical examinations. 1.9 average across all systems; respondents indicated low confidence in the privacy of pictures taken using the VoIP systems
Management of Requests for Information:	Determine if the company provides personal information when requested by legal authorities. Determine default settings for use of your personal information with third parties.	Do you think a complete and accurate consent to disclosure should be made to all users each time that information is requested or released? How sure do you feel that personal information will not be shared with other websites? Likert scale, 1-5 (1= not at all; 5= very) Do you think there should be restrictions to where your information is sent? How secure do you feel about your information not being sent to foreign countries? Likert scale, 1-5 (1= not at all; 5= very)	92% of respondents said yes, consent to disclosure should be made to all users each time information is requested or released. This is especially true as it relates to patient data – a HIPAA requirement. 2.2 average across all systems; respondents indicated low confidence that personal information would not be shared with other websites. 100% of respondents said yes, there should be restrictions that limit the sharing of information without consent. 1.9 average over all systems; respondents indicated low confidence that information would not be sent to foreign countries.

Evaluation Parameter	User Tasks	Questions	Results
Encryption Status	Determine the system encryption level. Determine if the encryption covers video-therapy sessions.	How would you rate the encryption of this VoIP system? Likert scale, 1-5 (1= not at all encrypted; 5= very encrypted) How important is encryption to you in order to make sessions private and secure during transmission? Likert scale, 1-5 (1= not at all important; 5= very important)	2.6 average across all systems; respondents indicated low-moderate confidence in the encryption level of the VoIP systems. 5.0 average; respondents ranked encryption as very important to assure privacy and security of video conferencing using VoIP systems.
Anti Virus/Anti- Spyware Protection:	Determine whose responsibility it is to prevent eavesdropping during a video conference with anti-virus/anti-spyware. Determine how secure a video conferencing session is and how much information can be transmitted to someone.	Should it be the user's or VoIP's responsibility to prevent eavesdropping during a video conference with a client? How secure do you feel that no one will listen in on your video conferencing session? Likert scale, 1-5 (1= not at all secure; 5= very secure)	42% VoIP 33% User 25% Both 2.4 average across all systems; respondents indicated low-moderate confidence that no one would listen in on video conferencing sessions.
User's Public Profile:	View your public profile. Determine what information the public can see.	Do you feel that the public should see less or more of your information than they can currently see? How confident do you feel that your information will only be accessible to those whom you have authorized to gain access? Likert scale, 1-5 (1= not at all confident; 5= very confident)	83% of respondents prefer less information be publicly available. 1.8 average across all systems; respondents indicated low confidence in information being accessible only to authorized individuals.
Caller Management (Allowing, removing, blocking)	Make a call to a simulated client. Determine how to block a caller.	How secure do you feel with your video conferencing options? Likert scale, 1-5 (1=not at all secure; 5=very secure) How certain do you feel that your blocked caller can no longer see your video session? Likert scale, 1-5 (1= not at all secure; 5= very secure	2.8 average across all systems; respondents were moderately secure with their video conferencing options. 2.8 average across all systems; respondents were moderately confident that a blocked caller could no longer see their video sessions.

Evaluation Parameter	User Tasks	Questions	Results
Audit System Activity	Determine if server logs are generated for audit trail purposes. Determine any other audit system activity on this VoIP system.	Do you think that server logs should be included in all VoIP systems? Do you believe it is necessary for video conferencing sessions to be audited?	83% respondents indicated that server logs should be included in all VoIP systems. 50% respondents stated yes; other respondents believed these are private sessions and should not be audited.
Overall Evaluation	Evaluate the system for privacy and security.	How secure/private do you think this system is if used for a video therapy session between you and your client? Likert scale, 1-5 (1= not at all secure/ private; 5= very secure/ private)	Overall across all systems: Average: 2.6 Median = 3.0; respondents were moderately confident in the security/privacy of the VoIP system for use in video therapy sessions. [Average for each system: System 1: 3.0; System 2: 2.0; System 3: 2.8]

***Table 2**: Evaluation Protocol and Results*

Qualitative Comments:

Qualitative comments by the respondents are summarized below. In general, the following themes emerged:

1. More than a password should be used to enter the VoIP system. The providers did not believe that just a username and password is enough to keep the system secure. Additional methods, such as asking for other information, biologic data, finger print, eye scan, or other verification methods should be used to maintain the confidentiality of information as it flows over the Internet. Also, a Virtual Private Network should be used to maintain privacy and security.
2. The respondents did not feel very confident that their video therapy session would be private. One respondent observed this may be no different than an in-person session with the patient where, sometimes, employees or other patients may be able to listen to a treatment session.
3. The respondents did not agree with VoIP companies' policies of sharing user information with other websites and foreign countries. The respondents believed information sharing could potentially lead to breakdowns in privacy and security of user information since many other countries do not have strict privacy and security policies such as HIPAA. Also, they did not understand why so much information sharing occurred with other websites and why the VoIP site did not take responsibility for the privacy and security policies on those websites.
4. All respondents felt that the privacy and security policies were very difficult to read and understand and were not certain that the policies were followed.
5. The respondents were critical of the encryption policies. Not all of the consumer-based, free VoIP systems investigated in this usability study indicated the use of encryption within their systems. Respondents had to search for the information in the systems' policies; once it was found it was difficult to tell if the video stream was encrypted. Personal information, email, and other data seemed to be encrypted, but some of the policies did not specify methods of encryption for video streams.

Limitations:

There are several limitations to the pilot study design; they include the following:

1. Only four respondents completed all tasks across systems. If more respondents were used to assess the VoIP systems many different opinions and answers to the questions may have emerged and may have changed the conclusions.
2. Only three consumer-based, free VoIP systems were included in the study. Even though only three systems were included, they are the most popular, free VoIP

systems available currently. However, expanding the types and numbers of systems would allow for results that may better represent the population under study.

3. The study was not deployed in simulated or authentic client and provider telerehabilitation environments. A future study may include use of the VoIP systems in a client/provider environment and obtain comments from both clients and providers on the perceived security and privacy of the treatment session.

Recommendations

There are several recommendations that if implemented, could lead to improved privacy and security for consumer-based VoIP systems.

Recommendations for VoIP Companies

The first set of recommendations is for the VoIP companies. They should provide a more secure entrance into the system. A username and password is not enough when health related information is being transferred across the Internet and across different countries and websites. As mentioned by the respondents, further security upon entering the system may include finger prints, eye scans, or biological data. Additionally, the system should be maintained across a Virtual Private Network (VPN). Impersonation of the system should be prevented. Some of the sites may be impersonated so that it looks like a user is logged into the real system but is actually in an impersonation system/website. When this occurs, impersonators can use some of the personal information collected for the wrong purpose. This happened to one of the systems researched. Each of the systems should have clear policies that describe the privacy and security of the video conferencing session and address in clear terms how they will:

- Restrict employees from listening for purposes other than to address technical problems
- Restrict information to other users
- Restrict retention of the session
- Provide a consent for disclosure to all users
- Prevent sharing of information with other websites, countries, and other third parties.
- Insure HIPAA compliance and enter into a business associate agreement with the provider or covered entity.

Recommendations for Providers

It is recommended that providers:

- Form a team (e.g., provider, risk manager, IT specialist) and use the checklist developed by Watzlaf, Moeini, & Firouzan, (2010) to review HIPAA compliance before using any videoconferencing system.
- Review the privacy and security policies of each system before use.
- Ask questions of the company that are not addressed in the policies.
- Develop clear, understandable privacy and security policies and incorporate the policies into a client consent form. Address questions as they pertain to HIPAA and the US Office of Civil Rights (OCR) requirements.

Recommendations for Clients/ Consumers

Clients/consumers can play an important role in advocating for security and privacy. It is recommended that they:

- Advocate for a readable, clear privacy and security policy either within the system consent/agreement of use or as part of the system policies.
- Ask questions about privacy and security when using any videoconferencing system.
- Know their privacy rights as they pertain to HIPAA and other US Office of Civil Rights requirements.

Conclusions

It is important to examine the privacy and security of any software system that is used to transmit or store health related information. With the new rules from the American Recovery and Reinvestment Act of 2009 (ARRA) and Title XIII of ARRA: Health Information Technology for Economic and Clinical Health Act (HITECH) in relation to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, breaches of protected health information must be disclosed to the covered entity upon 60 days after discovery from the Business Associate.

Are VoIP consumer-based, free software systems considered Business Associates? Some believe they are if they handle protected health information, and some believe they are no more than a conduit transmitting health information similar to the US postal service transporting the mail. However, if the VoIP companies are storing the video conferencing session between a client and provider, even for a short period of time, and if those sessions are linked to personal information about the client, the company should be considered a business

Associate and should comply with HIPAA requirements. This relationship should be stated in their policies in clear, understandable terms. Also, it is important for the provider who is considering using these systems to realize that they were not developed to provide video therapy sessions for healthcare purposes.

In a recent presentation, Dr. David Blumenthal,[1] expressed the need for developing an "Internet for Healthcare" to achieve a higher level of privacy and security across the Internet. The same could be said for the VoIP systems used over the Internet. There should be "VoIP for Healthcare," with a higher level of privacy and security for any type of health information being exchanged across the Internet, but especially for services delivered via telerehabilitation.

Systems designed specifically for telehealth purposes (e.g., VISYTER[2]; VidyoHealth[3]) assure providers that the services provided through these systems meet HIPAA requirements.

References

1. Blumenthal, D. (2012, May 11). Grand rounds: Bringing health information to life. Montefiore University Hospital, University of Pittsburgh Medical Center, Pittsburgh, PA, USA.
2. Watzlaf, V., Moeini, S, Matusow, L, & Firouzan, P. (2011). VOIP for telerehabilitation: A risk analysis for privacy, security and HIPAA compliance: Part II. International Journal of Telerehabilitation, 3(1), 4-10. doi: 10.5195/ijt.2011.6070
3. 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

1. David Blumenthal, MD, MD, MPP, is Chief Health Information and Innovation Officer, Partners HealthCare, and Samuel O. Their Professor of Medicine and Professor of Health Care Policy Massachusetts General Hospital/Harvard Medical School
2. http://www.rerctr.pitt.edu/PolicyConf/Doc/PF_Handouts/ParmantoPFppt.pdf
3. http://www.vidyo.com