

Assessing Telehealth Operational and Technology Security Risks to Privacy

**Prepared by the Center for Telehealth
University of New Mexico Health Sciences Center
July 2003**

INTRODUCTION

The purpose of this document is to provide an overview of potential operational and technology security risks to privacy in clinical telehealth interactions. It is not intended to outline all possible risks to privacy when utilizing telehealth technologies; rather it is meant to serve as a framework for assessing the risks that a telehealth program is most likely to encounter. Each program and organization involved in telehealth should conduct a thorough privacy risk assessment for each of their telehealth applications.

DOCUMENT ORGANIZATION

For ease of use, this document has been divided into two parts:

Part I – Technology Security Risks Assessment Overview -assesses the probability of a security breach based upon the technology utilized.

Part II- Assessing Telehealth Operational Risks to Privacy- provides an overview of the potential risks to privacy in telehealth encounters that are primarily due to operational factors.

Both parts include recommendations for minimizing risks to privacy in telehealth encounters.

Definitions are provided at the end of the document.

ACKNOWLEDGEMENT

Much of the content for Part II of this document has been adapted from “Protecting Privacy When Using Telehealth Technology in Healthcare”, a two volume report prepared by the Advanced Technology Institute for the US Department of Health and Human Services. For the full report please see:
http://tdrt.aticorp.org/privacydoc_vol1.html and
http://tdrt.aticorp.org/privacydoc_vol2.html

Part I - Technology Security Risks Assessment Overview

PREAMBLE

HIPAA regulations assess risks based on the probability (likelihood) of a security breach multiplied times the impact if a security breach occurs. HIPAA requires electronic systems and handlers of PHI data to make a reasonable attempt to secure PHI. Part I of this document assumes that disclosure of any type or amount of PHI would cause significant impact. Therefore, this section primarily assesses the probability of a security breach based upon the technology selection.

MATRIX OVERVIEW

Security Risks Categories

Technologies	Unauthorized Electronic Access to PHI	Unauthorized Electronic Disclosure of PHI	Data/Video Integrity Corruption
Videophone H.324 (See section 1 notes.)	Low	Low	Low
ISDN Interactive Video-H.320 (See section 2 notes.)	Low to Medium	Medium to High	Low
IP Interactive Video- H.323 (See section 3 notes.)	High	Medium to High	Medium
Store-and-Forward Technologies (See section 4 notes.)	High	High	High

SECTION 1 – Video phone H.324

Summary

Videophone (H.324) technology enables low quality interactive video connectivity over an analog telephone line, otherwise known as plain old telephone service (POTS). Since HIPAA regulations formally exclude POTS based technologies, videophone technology presents a low security risk in all three identified security risks categories. Some institutions may choose to define POTS based technologies as “Not Applicable”.

Unauthorized Electronic Access to PHI

Low

Although illegal use of telephone wiretaps could provide access to the audio portion of the conversation, HIPAA does not require security measures be taken to address POTS based technologies such as videophone, fax machines or

standard telephone conversations since the only legal threat of access exists when an individual obtains a court order to wiretap a line.

Unauthorized Electronic Disclosure of PHI

Low

The user should always be able to verbally verify the identity of the individual in the remote location. Since videophones only support point-to-point connections, it is improbable for a third party participant to unknowingly electronically join the video interaction.

Data/Video Integrity Corruption

Low

Videophone technology provides a consistent level of 15 fps video quality. The audio quality is equivalent to a standard telephone call. The user would be able to immediately identify any degradation in video quality or audio reception. A health provider should discontinue use of the videophone if video or audio quality impacts the provider's ability to provide high quality service.

SECTION 2 – ISDN Interactive Video H.320

Summary

ISDN Interactive Video (H.320) technology enables 'high' quality interactive video connectivity using a switched ISDN circuit. The circuit establishes dedicated bandwidth ensuring reliable video and audio quality. Most institutions agree that H.320 ISDN video conferencing subsist as a low risk form of telecommunications. However, users should assess the engineering design of the network to ensure that the connectivity is ISDN switched services from end point to end point.

Unauthorized Electronic Access to PHI

Low to Medium

An individual can illegally wiretap an ISDN circuit to access information traveling via the telecommunications circuit. However, in order to actually view/hear the two-way interactive video session the user would have to own relatively expensive codec equipment that could code and decode the video and audio transmission. Furthermore, most H.320 interactive video connections would incur significant errors if a wiretap occurred and likely disconnect. Therefore, most institutions consider the use of ISDN H.320 interactive video as a "reasonable" attempt to protect PHI. Most institutions consider this network arrangement "low" risk.

However, depending upon the engineering design of the network, the transmission may travel internally as an IP connection (see Section 3) and/or some networks allow network support individuals to remotely access and view interactive video sessions. There are two common mechanisms that allow technical support individuals to anonymously view sessions. First, some institutions design their networks so that all video sessions filter through a central hub that allows technical staff to view and hear interactive video sessions on an ad hoc basis. Conference participants would not be aware of the individual's decision to view the conference. Secondly, many video conferencing units maintain an IP based

data connection that allows authorized technical support staff to view the conference session from their desktop. Although audio is not transmitted, the technical support staff could view the video portion of the conference. Health care providers should check with the institution to identify if these potential security risks exist and make appropriate technical or contractual arrangements to protect PHI.

Unauthorized Electronic Disclosure of PHI **Medium to High**

When using H.320 interactive video technology, there are mechanisms in place that would allow for users to accidentally disclose PHI.

Systems often allow for the option of simultaneously offering a video stream session of the interactive videoconference. If the video stream feature is enabled, individuals can view and hear the videoconference using their web browser interface and a commonly available video player technology such as QuickTime, Real Player or Window Media. Users should check with technical staff to ensure all video streaming technologies are disabled for any conference that includes PHI.

Also, many institutions enable their interactive video systems to automatically answer incoming video connection calls. Although conference participants would be aware of any individual joining the conference, existing videoconference session participants/patients would temporarily be revealed. Most videoconference units have the option to disable this “auto answer” feature, as well as place the unit in a “do not disturb” mode.

Additionally, conference participants must be aware that any site participating in the conference maintains the capability of videotaping a conference without the knowledge of other conference participants. Users should address this potential technical security breach through operational protocols.

Video Integrity Corruption **Medium**

H.320 interactive videoconferencing technology provides a consistent level of 30 fps video quality. The audio quality supports real-time conversation between all users at a level that does not interfere with communication. A user would be able to immediately identify any degradation in video quality or audio reception that might impede a health care professional’s ability to provide treatment or care recommendations. A health provider should discontinue use of the technology if video or audio quality impacts the provider’s ability to provide high quality service.

All medical scopes used to support clinical applications in conjunction with the interactive video unit should be FCC approved and/or provide consistent quality of data/video necessary for the health professional to make an adequate assessment or diagnosis.

SECTION 3 – IP Interactive Video H.323

Summary

IP Interactive Video (H.323) technology enables interactive video connectivity using public Internet and/or private intranets. When traversing the public Internet, quality and security can be significantly impacted. Quality depends upon the bandwidth available on the Internet at any given point in time. Since users worldwide compete for Internet bandwidth, video connections traversing the public Internet may fluctuate in video and audio quality, as well as reliability. With regards to security issues, public Internet traffic remains easily accessible to individuals to sniff, monitor and “hack”. Therefore, videoconferences utilizing public Internet paths require technical and operational solutions to reasonably protect PHI.

Unauthorized Electronic Access to PHI

High

An individual with a little "know how" and commonly available equipment can easily access videoconferencing sessions that traverse the public Internet. Any videoconference session using the public Internet as their form of connectivity should either eliminate all PHI or work with technical support staff to employ virtual private networks (VPNs) or encryption technologies to protect PHI.

Most institutions consider videoconferencing sessions that utilize H.323 IP technology but do not traverse the public Internet as reasonably protected since the information remains on a “trusted” network. However, all institutions should not be considered “trusted” networks. For example, colleges and universities often use one network to host all applications. Therefore, student health clinics or other health facilities’ data using their own campus network (intranet) remain at risk since many students and others not involved in patient treatment possess access to the network.

Furthermore, some networks allow network support individuals to remotely access and view interactive video sessions. There are two common mechanisms that allow technical support individuals to anonymously view sessions. First, some institutions design their networks so that all video sessions filter through a central hub that allows technical staff to view and hear interactive video sessions on an ad hoc basis. Conference participants would not be aware of the individual’s decision to view the conference. Secondly, some video conferencing units also maintain an IP based data connection that allows authorized technical support staff to view the conference session from their desktop. Although audio is not transmitted, the technical support staff could view the video portion of the conference.

Unauthorized Electronic Disclosure of PHI

Medium to High

When using H.323 interactive video technology, there are mechanisms in place that would allow for users to accidentally disclose PHI.

Systems often allow for the option of simultaneously offering a video stream session of the interactive videoconference. If the video stream feature is enabled, individuals can view and hear the videoconference using their web browser interface and a commonly available off the shelf video player technology such as QuickTime, Real Player or Window Media. Users should check with technical staff to ensure all video streaming technologies are disabled for any conference that includes PHI.

Also, many institutions enable their interactive video systems to automatically answer incoming video connection calls. Although conference participants would be aware of any individual joining the conference, existing videoconference session participants/patients would temporarily be revealed. Most videoconference units have the option to disable this “auto answer” feature, as well as place the unit in a “do not disturb” mode.

Additionally, conference participants must be aware the any site participating in the conference maintains the capability of videotaping a conference without the knowledge of other conference participants. Users should address this potential technical security breach through operational protocols.

Video Integrity Corruption

Medium

H.320 interactive videoconferencing technology provides a consistent level of 30 fps video quality if sufficient bandwidth exists. The audio quality supports real-time conversation between all users at a level that does not interfere with communication. However, if adequate bandwidth is not available, quality depends upon the bandwidth available on the Internet at any given point in time causing video and audio quality to fluctuate. A user would be able to immediately identify any degradation in video quality or audio reception that might impede a health care professional’s ability to provide treatment or care recommendations.

All medical scopes used to support clinical applications in conjunction with the interactive video unit should be FCC approved and/or provide consistent quality of data/video necessary for the health professional to make an adequate assessment or diagnosis.

SECTION 4 – Store-and-Forward Technologies

Summary

The sharing of electronic information remains a critical part of today's health care process. This includes PHI data such as medical images, video clips, audio clips or medical records. The majority of electronic transmissions uses Internet Protocol (IP) and traverses the public Internet. The public Internet remains easily accessible to individuals to sniff, monitor and "hack". Therefore, data using public Internet paths require technical and operational solutions to reasonably protect PHI.

Unauthorized Electronic Access to PHI

High

An individual with a little "know how" and commonly available equipment can easily access data crossing the public Internet. Any health provider using the public Internet to electronically transfer data should either eliminate all PHI or work with technical support staff to employ virtual private networks (VPNs) or encryption or encoding technologies to protect PHI. The solution should be considered reasonable relative to the application and the information being shared. Also, users must remember that PHI residing on computer systems or other electronic devices remains at risk for unauthorized access. Users should consider technical security mechanisms such as procedures for emergency access, role based access and user based access, and message authentication.

Most institutions consider data electronically transferred internally (within their institution) as reasonably protected since the information remains on a "trusted" network. However, all institutions should not be considered "trusted" networks. For example, colleges and universities often use one network to host all applications. Therefore, student health clinics or other health facilities' data using their own campus network (intranet) remain at risk since many students and others not involved in patient treatment possess access to the network. Additionally, health information electronically transferred using email encumbers additional risks. Most institutions provide a mechanism for users to read their email from home or when traveling. Consequently, data intended to travel across an internal network is now using the public Internet to reach its destination. Therefore, any electronic transmissions containing PHI should be protected through at least one form of technology.

Additionally, users must require identification authorization for access to PHI stored on local computer systems or other electronic devices. Users should refer to their institution's computer use and HIPAA policies regarding measures required to minimize unauthorized electronic access to PHI on local systems.

Unauthorized Electronic Disclosure of PHI

Medium to High

When using electronic transmission technologies such as Email, users often unintentionally disclose PHI. Therefore, operational and technical solutions should exist to minimize a user's ability to accidentally disclose PHI.

Email and other store-and-forward technologies facilitate the disclosure of PHI. Users may incorrectly address an email, reply to all users or forward a received email with PHI. Such circumstances exemplify unauthorized electronic disclosure of PHI. If email or other forms of asynchronous transmission remain critical forms of communication for PHI, users must use encryption technologies or other solutions that require the intended recipient to enter a password or possess an electronic key to access the information.

Data Integrity Corruption

High

Users should implement measures to eliminate unauthorized access (See Section 4– Unauthorized Electronic Access to PHI). This step will contribute significantly to ensuring data integrity of electronically transmitted PHI. Users should also consider technical security mechanisms such as automatic logoff, event reporting, encryption, and audit trails. Furthermore, users should refer to their institution’s computer use and HIPAA policies regarding measures required to assure data integrity for PHI on local systems.

Part II

Assessing Telehealth Operational Risks to Privacy

PREAMBLE

There are numerous potential risks to privacy in any health care activity that requires the exchange of PHI between organizations or individual providers. The potential for PHI to be exposed when organizations or individual providers cooperate in a telehealth/telemedicine interaction may be greater than face-to-face interactions, particularly when telehealth activities are not integrated into an organization's usual practice patterns. Though the risks discussed in this document may apply to any health care activity that requires the exchange of PHI, there are a few risks unique to telehealth. For example, patients generally know who is in an examining room with them. In the case of telehealth, patients may not be aware of third parties who are off camera at the consulting site.

Part II of this document discusses risks associated with clinical telehealth interactions, i.e. telehealth encounters for treatment purposes. It does not discuss educational or other uses of telehealth, such as case presentations for educational purposes, nor does this section address e-mail correspondence between providers and patients, home health, or web based applications. The two types of telehealth technologies that this section pertains to are: 1) interactive videoconferencing and 2) store-and-forward technologies.

There are three types of interactive technology platforms typically used for telehealth encounters: videophone (H.324), ISDN interactive video (H.320), and IP interactive video (H. 323). Though each of these technologies has unique security risks (see Part I - Technology Security Risks Assessment Overview), the operational issues are similar for all three interactive technology platforms. In general, there are fewer operational risks, though greater security risks, associated with store-and-forward applications since communication usually takes place directly between providers. Scheduling intermediaries are not usually required for store-and-forward consultations and technical personnel are generally not involved in the actual telehealth interaction, though they may have access to the communication systems that support the store-and-forward applications.

TELEHEALTH ENCOUNTER PROCESS

Breaches of privacy may occur during any stage of a telehealth encounter. Most telehealth interactions will have three phases: 1) arranging for the interaction, 2) conducting it, and 3) documenting the result of the telehealth encounter. Each phase of the encounter may contain several steps:

Arranging Telehealth Encounter – 1) obtain patient agreement/permission to participate, 2) obtain consultant agreement to participate, 3) share patient history with consultant, 4) schedule patient visit

Conducting Telehealth Encounter – 1) review patient history, 2) initiate patient involvement, 3) initiate encounter, determine diagnosis/plan of care, 4) provide feedback to patient, 5) provide feedback to staff at remote site/referring provider

Documenting Telehealth Encounter – Document care in patient record

MATRIX OVERVIEW

(The matrix below identifies 7 common telehealth operational risks and indicates where in the telehealth encounter each risk is likely to occur.)

Risk	Arranging telehealth encounter	Conducting telehealth encounter	Documenting telehealth encounter
<i>Differences in operational procedures between cooperating locations could cause PHI exposure (See section A notes)</i>	√	√	√
<i>3rd party may intercept or view PHI (without knowledge of participants) (See section B notes)</i>	√	√	√
<i>3rd party may see PHI (in form of handwritten notes, printouts, etc.) that has not been secured in files or destroyed (See section C notes)</i>	√	√	√
<i>PHI may be exposed to 3rd parties since many authorized individuals and sites may be involved in establishing the appointment (See section D notes)</i>	√		
<i>3rd party may overhear conversation where PHI is expressed (See section E notes)</i>	√	√	
<i>Individuals at either site may misrepresent their identities (See section F notes)</i>	√	√	
<i>Patient may not realize that the consulting provider retains PHI in his/her possession (See section G notes)</i>	√		√

Section A

Risk: Differences in operational procedures between cooperating locations could cause PHI exposure

The risk for privacy breaches is greatest in settings in which telehealth is not fully integrated into the clinical operations of the participating sites. It is important that cooperating sites develop and agree on shared operational procedures and that these procedures are compatible across sites. Operational protocols should define what information will be exchanged between cooperating locations and how that information will be exchanged and protected. Organizations utilizing telehealth should require PHI protection as part of their contracts and Business Associates Agreements with outside organizations that provide services to the telemedicine/telehealth environment.

Section B

Risk: 3rd party may intercept or view PHI (without knowledge of participants)

In addition to the various security risks to PHI outlined in Part I of this document, there are operational risks to PHI when participating in telehealth activities. For example, personnel could be present at the consulting site without the patient being aware of their presence. Telehealth encounters could be videotaped at the consulting site and later distributed without the patient's knowledge. Operational policies and procedures such as panning the consulting site with the camera and introducing all personnel present including the technical staff should be developed and strictly enforced. Personnel not assisting with the care of the patient should not be present in the consult room without patient authorization and telehealth consultations should not be videotaped without patient permission.

It is also important to ensure that contracts and Business Associates Agreements with providers of technical services (e.g. videoconferencing bridges, videoconferencing services, technical support for computer/communications technologies, etc.) impose the same PHI protection responsibilities that are in place for site personnel.

It is possible for PHI to be intercepted in the process of scheduling consultations or exchanging necessary patient information with the consultant prior to the telehealth encounter. Physical security measures should be developed to protect PHI used in delivering care from unauthorized access. Procedures to ensure the privacy of incoming and outgoing materials should be implemented in order to limit the risk of third parties intercepting or viewing PHI.

If store-and-forward applications are used to exchange PHI, organizations should require identification authorization for access to systems containing PHI.

Section C

Risk: 3rd party may see PHI (in form of handwritten notes, printouts, etc.) that has not been secured in files or destroyed

Organizations providing telehealth services should develop policies and procedures to define the appropriate distribution, filing and maintenance of consent forms, appointment scheduling records and medical records. Consulting providers should open and work with documents only in an appropriate setting and destroy patient information if referrals

are terminated. Interim documentation of telehealth encounters, such as hand written notes, should be treated with the same care as medical record components. Information that is not required for either of the sites' medical records or support of the remote telehealth site's appointment should be destroyed.

Section D

Risk: PHI may be exposed to 3rd parties since many authorized individuals and sites may be involved in establishing the appointment

In order to reduce the risk of PHI being exposed to third parties, implement methods to reduce the number of steps and individuals required to schedule a telehealth appointment. Limit the use of, disclosure of, and request for PHI to the minimum amount of information necessary to accomplish the purpose of the use, disclosure, or request.

Section E

Risk: 3rd party may overhear conversation where PHI is expressed

Safeguard oral communications by ensuring that reasonable efforts are being made to avoid being overheard when sharing PHI such as soundproofing consult rooms, keeping the telehealth system's speaker volume down and closing the doors to telehealth rooms at both the patient and consulting sites.

Since technical support staff may overhear PHI during telehealth encounters, technical staff should receive HIPAA training and follow all privacy and confidentiality policies of the institution. If using outside technical services (e.g. videoconferencing bridges, videoconferencing services, technical support for computer/communications technologies, etc.) develop contracts and/or Business Associates Agreements that impose the same PHI protection responsibilities that are in place for site personnel.

Section F

Risk: Individuals at either site may misrepresent their identities

Develop procedures to confirm the identities of participants. This is especially important when there is no previously established relationship between participants and their identities cannot be confirmed verbally or by sight. Individual sites should be easily identifiable by signage in the telehealth rooms.

Section G

Risk: Patient may not realize that the consulting provider retains PHI in his/her possession

Patients should be fully informed about all aspects of the telehealth interaction.

DEFINITIONS

Bandwidth - The amount of data that can be transmitted in a fixed amount of time. For digital devices the bandwidth is usually expressed in bits per second (bps) or bytes per second.

Clinical telehealth interaction – A telehealth encounter for treatment purposes.

Codec – (abbreviation of **coder/decoder**) a device that encodes or decodes a signal.

Encryption – The translation of data into a secret code. To read an encrypted file, you must have a secret key or password that enables you to decrypt it. Unencrypted data is called *plain text*; encrypted data is referred to as *cipher text*.

Encoding – An algorithm for the compression of files based on the frequency of occurrence of a symbol in the file that is being compressed

FPS – (abbreviation of frames per second) a measure of how much information is used to store and display motion video. The more frames per second (fps), the smoother the motion appears. Television in the U.S displays 30 frames per second (*60 fields per second*). In general, the minimum fps needed to avoid jerky motion is about 30.

Intranet - A network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization

ISDN – (abbreviation of *integrated services digital network*) an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires. There are two types of ISDN: Basic Rate (BRI) ISDN and Primary Rate ISDN

IP – (abbreviation of *Internet Protocol*) specifies the format of data packets and the addressing scheme.

Interactive videoconferencing (IATV) - Interactive video conferencing is the transmission of real-time audio and video between two or more locations.

PHI – (abbreviation for protected health information)

POTS – (abbreviation of plain old telephone service); the analog standard used to provide telephone service to most homes

Store-and-forward (S&F) - Asynchronous electronic exchange of patient information, images, or data for the purpose of providing or supporting clinical care at a distance

Videophone – H.324 interactive video conferencing technology that utilizes an analog phone line to transmit audio and video using low bandwidth technology.

VPN – (abbreviation of virtual private network) a group of two or more computers or other system types linked together using public wires, such as the Internet, to connect the nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.